Release Notes for the Cisco ASR 903 RouterF

February 3, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-26630-09

Cisco IOS XE 3S Release Notes for the Cisco ASR 903 Router

CONTENTS

Release Notes for the Cisco ASR 903 Router

The Cisco ASR 903 Router runs the Cisco IOS XE software beginning with Release 3.5.0S. This document provides information about the IOS XE software release for the Cisco ASR 903 Router beginning with Release 3.6(0)S.

Note For information about Cisco IOS Release 3.5, see the Release Notes for Cisco IOS XE Release 3S.

The following sections provide an overview of the Cisco ASR 903 Router and Cisco IOS XE releases:

Cisco ASR 903 Router Overview

The Cisco ASR 903 Router is a fully-featured routing platform designed for the cost-effective delivery of converged mobile and business services. With full redundancy, shallow depth, low power consumption and high service scale, this 3-rack-unit (3RU) router is optimized for small aggregation and remote point-of-presence (POP) applications. The Cisco ASR 903 Router provides a rich and scalable feature set of Legacy, Timing, Carrier Ethernet, Layer 2 VPN (L2VPN) and Layer 3 VPN (L3VPN) services in a compact package.

The Cisco ASR 903 Router is a fully modular platform with support for 6-Interface Modules (IMs), two Route Switch Processor (RSP) slots, two power supplies and redundant fans. Cisco offers a wide choice of LAN and WAN interfaces available in speeds ranging from nxDS0 to 10 Gigabit Ethernet. The design of the Cisco ASR 903 Router delivers in-box hardware redundancy for all hardware components and supports software redundancy with In Service Software Upgrade (ISSU) and Non-Stop Forwarding (NSF) support.

Text Part Number: OL-26630-05

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

Software Licensing Overview

The Cisco ASR 903 Router offers the following base licenses:

- Metro Services
- Metro IP Services
- Metro Aggregation Services

The Cisco ASR 903 Router offers the following additional feature licenses:

- ATM
- IEEE 1588-2008 Boundary Clock/Master Clock
- OC-3 Port License

Note These features require a software license to use.

For more information about each software license including part numbers, see the Cisco ASR 903 Router Datasheet. For instructions on how to install licenses on the Cisco ASR 903 Router, see the Software Activation Configuration Guide, Cisco IOS XE Release 3S.

Documentation Roadmap

To view other documents for the Cisco ASR 903 Router, see the Cisco ASR 903 Router Documentation Roadmap.

Determining the Software Version

You can use the following commands to verify your software version:

- Consolidated Package—**show version**
- Individual sub-packages—**show version installed** (lists all installed packages)

Upgrading to a New Software Release

Only Cisco IOS XE 3S consolidated packages can be downloaded from Cisco.com; users who want to run the router using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

For information about upgrading to a new software release, see the *Cisco ASR 903 Router Chassis Software Configuration Guide* at http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.7.0S/ASR903-Chassis-SW-39.html.

Supported ROMmon Versions

15.3(2r)S is the recommended ROMmon version for IOS XE 3.5, 3.6, 3.7, 3.8, and 3.9 software releases.

Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected:

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

MIB Support

This section describes the MIB support on the Cisco ASR 903 Router.

- Table 1 summarizes the supported MIBs on the Cisco ASR 903 Router:

Table 1 Supported MIBs

Supported MIBs		
BGP4-MIB (RFC 1657)	CISCO-IMAGE-LICENSE-MGMT-MIB	MPLS-LDP-STD-MIB (RFC 3815)
CISCO-BGP-POLICY-ACCOUNTING-MIB	CISCO-IMAGE-MIB	MPLS-LSR-STD-MIB (RFC 3813)
CISCO-BGP4-MIB	CISCO-IPMROUTE-MIB	MPLS-TP-MIB
CISCO-BULK-FILE-MIB	CISCO-LICENSE-MGMT-MIB	MSDP-MIB
CISCO-CBP-TARGET-MIB	CISCO-MVPN-MIB	NOTIFICATION-LOG-MIB (RFC 3014)
CISCO-CDP-MIB	CISCO-NETSYNC-MIB	OSPF-MIB (RFC 1850)
CISCO-CEF-MIB	CISCO-OSPF-MIB (draft-ietf-ospf-mib-update-05)	OSPF-TRAP-MIB (RFC 1850)
CISCO-CLASS-BASED-QOS-MIB	CISCO-OSPF-TRAP-MIB (draft-ietf-ospf-mib-update-05)	PIM-MIB (RFC 2934)
CISCO-CONFIG-COPY-MIB	CISCO-PIM-MIB	RFC1213-MIB
CISCO-CONFIG-MAN-MIB	CISCO-PROCESS-MIB	RFC2982-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-PRODUCTS-MIB	RMON-MIB (RFC 1757)
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-PTP-MIB	RSVP-MIB
CISCO-ENHANCED-MEMPOOL-MIB	CISCO-RF-MIB	SNMP-COMMUNITY-MIB (RFC 2576)
CISCO-ENTITY-ALARM-MIB	CISCO-RTTMON-MIB	SNMP-FRAMEWORK-MIB (RFC 2571)
CISCO-ENTITY-EXT-MIB	CISCO-SONET-MIB	SNMP-MPD-MIB (RFC 2572)
CISCO-ENTITY-FRU-CONTROL-MIB	CISCO-SYSLOG-MIB	SNMP-NOTIFICATION-MIB (RFC 2573)
CISCO-ENTITY-SENSOR-MIB	DS1-MIB (RFC 2495)	SNMP-PROXY-MIB (RFC 2573)
CISCO-ENTITY-VENDORTYPE-OID-MIB	ENTITY-MIB (RFC 4133)	SNMP-TARGET-MIB (RFC 2573)
CISCO-FLASH-MIB	ENTITY-SENSOR-MIB (RFC 3433)	SNMP-USM-MIB (RFC 2574)
CISCO-FTP-CLIENT-MIB	ENTITY-STATE-MIB	SNMPv2-MIB (RFC 1907)
CISCO-IETF-ISIS-MIB	EVENT-MIB (RFC 2981)	SNMPv2-SMI
CISCO-IETF-PW-ATM-MIB	ETHERLIKE-MIB (RFC 3635)	SNMP-VIEW-BASED-ACM-MIB (RFC 2575)
CISCO-IETF-PW-ENET-MIB	IF-MIB (RFC 2863)	SONET-MIB
CISCO-IETF-PW-MIB	IGMP-STD-MIB (RFC 2933)	TCP-MIB (RFC 4022)
CISCO-IETF-PW-MPLS-MIB	IP-FORWARD-MIB	TUNNEL-MIB (RFC 4087)

Table 1 Supported MIBs

Supported MIBs		
CISCO-IETF-PW-TDM-MIB	IP-MIB (RFC 4293)	UDP-MIB (RFC 4113)
CISCO-IF-EXTENSION-MIB	IPMROUTE-STD-MIB (RFC 2932)	
CISCO-IGMP-FILTER-MIB	MPLS-LDP-GENERIC-STD-MIB (RFC 3815)	

Table 2 summarizes the unverified and supported MIBs on the Cisco ASR 903 Router.

Table 2 Unverified and Supported MIBs

Unverified MIBs		
ATM-MIB	CISCO-IETF-DHCP-SERVER-EXT-MIB	EXPRESSION-MIB
CISCO-ATM-EXT-MIB	CISCO-IETF-MPLS-TE-P2MP-STD-MIB	HC-ALARM-MIB
CISCO-ATM-IF-MIB	CISCO-IETF-PPVPN-MPLS-VPN-MIB	HC-RMON-MIB
CISCO-ATM-PVC-MIB	CISCO-IP-STAT-MIB	IEEE8021-CFM-MIB
CISCO-ATM-PVCTRAP-EXTN-MIB	CISCO-IPSLA-ETHERNET-MIB	IEEE8021-CFM-V2-MIB
CISCO-BCP-MIB	CISCO-L2-CONTROL-MIB	IEEE8023-LAG-MIB
CISCO-CALLHOME-MIB	CISCO-LAG-MIB	INT-SERV-GUARANTEED-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-MAC-NOTIFICATION-MIB	INTEGRATED-SERVICES-MIB
CISCO-CONTEXT-MAPPING-MIB	CISCO-MEMORY-POOL-MIB	MPLS-L3VPN-STD-MIB (RFC 4382)
CISCO-EIGRP-MIB	CISCO-NHRP-EXT-MIB	MPLS-LDP-ATM-STD-MIB (RFC 3815)
CISCO-ERM-MIB	CISCO-NTP-MIB	MPLS-LDP-MIB
CISCO-ETHER-CFM-MIB	CISCO-PING-MIB	MPLS-TE-STD-MIB
CISCO-ETHERLIKE-EXT-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	MPLS-VPN-MIB
CISCO-EVC-MIB	CISCO-RTTMON-ICMP-MIB	NHRP-MIB
CISCO-HSRP-EXT-MIB	CISCO-RTTMON-IP-EXT-MIB	RFC2006-MIB (MIP)
CISCO-HSRP-MIB	CISCO-RTTMON-RTP-MIB	RMON2-MIB (RFC 2021)
CISCO-IETF-ATM2-PVCTRAP-MIB	CISCO-SNMP-TARGET-EXT-MIB	SMON-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	CISCO-TCP-MIB	VRRP-MIB
CISCO-IETF-BFD-MIB	CISCO-VRF-MIB	
CISCO-IETF-DHCP-SERVER-MIB	ETHER-WIS (RFC 3637)	

MIB Documentation

The following resources provide more detail about MIBs on the Cisco ASR 903 Router:

- Cisco ASR 903 Router MIB Guide—For information about the Cisco ASR 903 Series Router product implementation of the MIB protocol, see *Cisco ASR 903 Series Aggregation Services Router MIB Specifications Guide* at the following location:

  http://www.cisco.com/en/US/docs/wireless/asr_900/mib/guide/asr903mib.html

- MIB Locator—To locate and download MIBs for selected platforms, Cisco IOS and Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following location:

  http://tools.cisco.com/ITDIT/MIBS/servlet/index

  To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at the following location:

  http://tools.cisco.com/RPF/register/register.do

Open Source License Notices

For a listing of the license notices for open source software used in Cisco IOS XE 3S Releases, see the documents accessible from the License Information page at the following location:

http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

2

New Features in Cisco IOS XE 3.6S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE Release 3.6S.

Note Cisco IOS XE 3.6S inherits all supported features from Cisco IOS Release 3.5, which is not described in this document. For more information about Cisco IOS Release 3.5, see the Release Notes for Cisco IOS XE Release 3S.

This chapter includes the following sections:

New Hardware Features in Cisco IOS XE Release 3.6(2)S

The IOS XE 3.6(2)S Release for the Cisco ASR 903 Router does not introduce any new hardware features.

New Hardware Features in Cisco IOS XE Release 3.6(1)S

The IOS XE 3.6(1)S Release for the Cisco ASR 903 Router does not introduce any new hardware features.

New Hardware Features in Cisco IOS XE Release 3.6S

The IOS XE 3.6(0)S Release for the Cisco ASR 903 Router introduces support for the following hardware features:

- New SFP modules—This release introduces support for the following SFP modules:
  - 1000M SFP-DWDM-SFP
  - 1000M SFP-CWDM
  - 1000M SFP - GLC-ZX-SMD
  - 1000M SFP - GLC-SX-MMD
  - 1000M SFP - GLC-LH-SMD
  - ONS-SI-155-SR-MM
  - ONS-SI-155-I1
  - ONS-SI-155-L1
  - ONS-SI-155-L2
- 4-Port OC3/STM-1 or 1-Port OC12/STM-4 Interface Module—This release introduces support for the A900-IMA4OS interface module. This combo module supports one of four modes: 4xOC3, 4xSTM-1, 1xOC12, and 1xSTM-4. The module supports SDH framing and HDLC encapsulation.

Note The A900-IMA4OS Interface Module requires a license for use. For more information about supported licenses, see Software Licensing Overview, page 2.

Note IOS XE Release 3.6 for the offers a limited set of software features for the A900-IMA4OS Interface Module. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html

New Software Features in Cisco IOS XE Release 3.6(2)S

The IOS XE 3.6(2)S Release for the Cisco ASR 903 Router does not introduce any new software features.

New Software Features in Cisco IOS XE Release 3.6(1)S

The following are the new software features introduced in Cisco IOS XE Release 3.6(1)S:

- OC-3 Interface Module Software Features—Release 3.6(1) introduces support for PPP and MLPPP the OC-3 interface module. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/OC_Ifc_Module.html
  - http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/pseudowire.html

  - http://www.cisco.com/en/US/docs/ios/ios_xe/atm/configuration/guide/xe_3s/atm_xe_3s_book.html
  - http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_media-ind_multi_ppp.html
  - http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_async_slip_ppp.html

- PPP MRRU Negotiation Configuration—Introduces support for the **ppp multilink mrru** command, which allows you to specify a Maximum-Receive-Reconstructed-Unit (MRRU) value on MLP interfaces and member links after a change in the MTU value on the interface. For details about this feature, see http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_pppmlp_mrru_neg.html.
- ACFC and PFC Support on Multilink Interfaces—Using the Address and Control Field Compression (ACFC) and PPP Protocol Field Compression (PFC) Support on Multilink Interfaces feature, you can control the negotiation and application of the Link Control Protocol (LCP) configuration options for ACFC and PFC.

  This release introduces support for ACFC and PFC support on serial interfaces on the T1/E1 and optical interface modules. This feature includes support for the following commands:

  - **ppp acfc local** {**request** | **forbid**}
  - **ppp acfc remote** {**apply** | **reject** | **ignore**}
  - **ppp pfc local** {**request** | **forbid**}
  - **ppp pfc remote** {**apply** | **reject** | **ignore**}

  For more information about configuring ACFC and PFC, see the following documents

  - http://www.cisco.com/en/US/partner/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgsip.html#wp1372108
  - http://www.cisco.com/en/US/partner/docs/routers/7600/install_config/flexwan_config/features.html#wp256581

- Egress QoS policies on main physical interface for port shaping + H-policies on EFP—Previous releases did not support QoS policies on interfaces configured with an Ethernet Flow Point (EFP) or port-channel member links with EFPs. This release introduces support for hierarchical QoS policies on EFP interfaces. For more information about how to configure QoS on EFP interfaces, see

  http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html

- Switch Port Analyzer—Release 3.6.1 introduces support for Switch Port Analyzer (SPAN) on physical interfaces. The following commands are supported:

  - **monitor session** {*session_number*} {**source** {**interface** *slot/port*}} [, | - | **rx** | **tx** | **both**]
  - **monitor session** {*session_number*} {**destination** {**interface** *type/num*} [, | -]}

  For more information about SPAN, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/SPAN.html

- Support for MPLS Labels with PTP traffic- This release introduces support for MPLS labels with PTP Delay-Request packets. The following encapsulation types are supported:

  - VPN
  - BGP IPv4
  - LDP
  - FRR

  The router adds time stamps to MPLS-encapsulated PTP packets by default.

- Reverse Path Forwarding failure handling—This release introduces support for the **platform multicast rpf_fail_handling enable** command. The Cisco ASR 903 Router hardware does not handle RPF fail packets default; you can use this command to enable RPF fail packets handling.

New Software Features in Cisco IOS XE Release 3.6S

The following are the new software features introduced in Cisco IOS XE Release 3.6S:

Note Many of the features supported on the Cisco ASR 903 Router require a license for use. For more information about supported licenses, see Software Licensing Overview, page 2.

- Any Transport over MPLS (AToM)—ATM AAL5 over MPLS (AAL5oMPLS)—The AAL5 Transport over MPLS feature provides an ATM permanent virtual circuit (PVC) transport service for transporting AAL5 PDUs across an IP/MPLS backbone with rate-limit policing and configurable PVC priority value. A dynamic MPLS tunnel is configured to enable label imposition and disposition of encapsulated ATM PDUs transported between two edge routers having a Label Distribution Protocol (LDP) neighbor relationship. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-2s/mp-any-transport.html
  - http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_any_transport_xe.html
  - http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html
  - http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html
- BFD IPv6 Encapsulation—This feature introduces support for IPv6 addresses with the BFD protocol. For details about this feature, see http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html
- BGP PIC Edge for IP/MPLS—This feature introduces support for BGP PIC Edge for IP/MPLS for sub-second convergence for IP and MPLS-VPN. For details about this feature, see:
  - http://www.cisco.com/en/US/partner/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/asr903/irg-xe-3s-asr903-book.html
  - http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_bgp_mp_pic.html
  - http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2mt/irg-bgp-mp-pic.html
- CFM over EFP interface with xconnect—This feature provides support for IEEE 802.1ag draft 8.1-compliant CFM functionality on pseudowire & VFI interfaces. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/CFM_EFP_xconnect.html
  - http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html
- CFM on Port-Channel Interfaces—This feature provides support for IEEE 802.1ag (CFM) on port-channel interfaces for end-to-end connectivity fault management on Ethernet networks. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm.html

  - http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html
  - http://www.cisco.com/en/US/partner/docs/ios-xml/ios/cether/configuration/xe-3s/ce-cfm.html
- Class-based QoS MIB—This feature introduces support for the class-based QoS MIB. For details about this feature, see http://www.cisco.com/en/US/docs/wireless/asr_900/mib/guide/asr903mib.html
- Egress QoS Marking—This feature introduces support for QoS marking on egress interfaces. For details about this feature, see http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html
- Egress QoS Policing—This feature introduces support for QoS policing on egress interfaces. For details about this feature, see http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html
- E-OAM-CFM CCM Hardware Offload—The router automatically offloads processing of Continuity Check (CC) messages if the CC interval is less than 1 second.
- H-VPLS N-PE Redundancy for MPLS Access—This feature allows user provider (U-PE) devices to be dual-homed to network provider edge (N-PE) devices in a loop-free topology with MPLS as the access/aggregation domain. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/12-2sy/mp-hvpls-npe-red.html
  - http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-3s/mp-hvpls-npe-red.html
- IPv6 Quality of Service Classification—This feature allows you to define traffic classes, create and configure traffic policies (policy maps), and attach those traffic policies to interfaces. The Cisco ASR 903 Router supports classification of IPv6 traffic based on DSCP or Precedence values on ingress and egress interfaces. For details about this feature, see
  - http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/xe-3s/ip6-qos.html
  - http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html
- IPv6 Quality of Service Marking—This feature introduces support for marking IPv6 traffic with DSCP or Precedence values. IPv6 QoS is supported on ingress and egress interfaces. For details about this feature, see
  - http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-qos_xe.html
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-qos.html
  - http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html
- ISIS IPv4 Loop Free Alternate Fast ReRoute (LFA FRR) for VPLS Core—IPFRR (IP Fast ReRoute) is a set of technologies used in order to rapidly converge traffic flows around link and/or node failures. For details about this feature, see http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_ipv4_lfafrr.html
- ITU-T G.8032 Ethernet Ring Protection Switching—This feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that there are no loops within the ring at the Ethernet layer. The loops

are prevented by blocking either a pre-determined link or a failed link. For details about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/ce-g8032-ering-pro.html

- L2 ACL on Service Instance—This is a security feature which customers can apply to an EVC interface to filter packets based on their MAC address. For details about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/ce-l2acl-evc.html
- L2PT - Layer 2 Protocol Tunneling on Trunk Ports—Layer 2 protocol tunneling makes control protocol PDUs such as STP, CDP, and VTP, transparent to the service provider cloud when passing traffic through trunk ports. For details about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/wan_lserv/configuration/xe-3s/wan-lserv-xe-3s-book.html
- MLPPP - Multilink PPP—Multilink PPP (also referred to as MP, MPPP, MLP, or Multilink) provides a method for spreading traffic across multiple physical WAN links and is described in RFC1990. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_media-ind_multi_ppp.html

Note Limitations apply when configuring MLPPP. For more information, see Chapter 2, "Restrictions and Caveats in Cisco IOS XE 3.6S Releases."

- MPLS Traffic Engineering (TE) - Fast Reroute (FRR) Link and Node Protection—This feature introduces support for MPLS Traffic Engineering (TE) - Fast Reroute (FRR) Link and Node Protection. For details about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-frr-node-prot.html
- Multiple Matching Commands—This feature introduces support for multiple **match** or **match-any** commands in a given QoS class-map. For details about this feature, see http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html
- Port-Shaper and LLQ in the presence of EFPs—This feature allows you to create a QoS policy to shape traffic across all EFPs on a given physical port. —For details about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-ehqos-pshape.html
- PPP—This feature introduces support for PPP, which provides a method for transmitting datagrams over serial point-to-point links. For details about this feature, see http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_async_slip_ppp.html
- Static Route Support for BFD over IPv6—This feature introduces support for static routes for BFD using IPv6 addressing. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/xe-3s/ip6-bfd-static-xe.html
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html
- Static VPLS over MPLS-TP—This feature introduces support for static VPLS over MPLS-TP. For details about this feature, see http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html
- STM-1 support—This feature adds support for STM1 mode on Cisco ASR 903 Router in concatenated and channelized mode to the DS1 level. For details about this feature, see http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html

- Support for Low Latency Queuing on Multiple EFPs—This feature allows you to apply a QoS policy for Low Latency Queuing to multiple EFP interfaces. For details about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-ehqos-pshape.html.
- Support for Weighted Random Early Detection—This feature introduces support for Weighted Random Early Detection (WRED) for congestion avoidance on egress interfaces. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/ios-xml/ios/qos_conavd/configuration/xe-3s/qos-conavd-diffserv-wred.html
  - http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_wred.html
  - http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00805b9497.html
  - http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html
- Y.1731 Performance Monitoring—Y.1731-PM provides a standards-based Ethernet performance monitoring function, which encompasses measurement of Ethernet frame delay, frame delay variation, frame loss, and frame throughput as outlined in the ITU-T Y-1731 specification and interpreted by the Metro Ethernet Forum (MEF) standards group. For details about this feature, see:
  - http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/ce-y1731-perfmon.html
  - http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_y1731-perfmon.html

New Features in Cisco IOS XE 3.7S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE Release 3.7S.

Note Cisco IOS XE 3.7S inherits all supported features from Cisco IOS Release 3.5, which is not described in this document. For more information about Cisco IOS Release 3.5, see the Release Notes for Cisco IOS XE Release 3S.

This chapter includes the following sections:

New Hardware Features in Cisco IOS XE Release 3.7(4)S

The IOS XE 3.7(4)S Release for the Cisco ASR 903 Router does not introduce any new hardware features.

New Hardware Features in Cisco IOS XE Release 3.7(3)S

The IOS XE 3.7(3)S Release for the Cisco ASR 903 Router does not introduce any new hardware features.

New Hardware Features in Cisco IOS XE Release 3.7(2)S

The IOS XE 3.7(2)S Release for the Cisco ASR 903 Router does not introduce any new hardware features.

New Hardware Features in Cisco IOS XE Release 3.7(1)aS

The IOS XE 3.7(1)aS Release for the Cisco ASR 903 Router introduces the following hardware features:

- AC Power Supply—Release 3.7(1)aS3.7(1)aS introduces support for the AC power supply. For more information about the AC power supply, see the *Cisco ASR 903 Hardware Guide*.

New Hardware Features in Cisco IOS XE Release 3.7(0)S

Release 3.7 introduces support for the ONS-SC-155-EL SFP module.

New Software Features in Cisco IOS XE Release 3.7(4)S

The IOS XE 3.7(4)S Release for the Cisco ASR 903 Router does not introduce any new software features.

New Software Features in Cisco IOS XE Release 3.7(3)S

The IOS XE 3.7(3)S Release for the Cisco ASR 903 Router does not introduce any new software features.

New Software Features in Cisco IOS XE Release 3.7(2)S

The IOS XE 3.7(2)S Release for the Cisco ASR 903 Router does not introduce any new software features.

New Software Features in Cisco IOS XE Release 3.7(1)aS

Release 3.7(1) introduces support for QoS policies on egress MLPPP interfaces on the T1/E1 interface module. For more information about how to configure QoS policies on MLPPP interfaces, see the *Cisco ASR 903 Router Chassis Configuration Guide, Release 3.7*.

New Software Features in Cisco IOS XE Release 3.7(0)S

The following are the new software features introduced in Cisco IOS XE Release 3.7(0)S:

- BGP Graceful Shutdown—The BGP Graceful Shutdown feature reduces or eliminates the loss of traffic along a link being shut down for maintenance. Routers always have a valid route available during the convergence process. This feature is used primarily for maintenance on a link between a PE and CE. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-grace-shut.html.
- Channelization Support—This release introduces support for channelization on the OC-3 interface module using the **channel-group** command. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.7.0S/ASR903-Chassis-SW-37.html.
- DHCP Option 82—In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on a switch, a subscriber device is identified by the switch port through which it connects to the network in addition to its MAC address. Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/dhcp82.html.
- DHCP Snooping—DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/dhcp82.html.
- Dynamic ARP Inspection—Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the bridge-domains and on the router. If the ARP packet is received on a trusted interface, the router forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/dynarp.html.
- E2E Transparent Clocking—A transparent clock is a network device such as a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of timing calculations. The transparent clock ports have no state because the transparent clock does not need to synchronize to the grandmaster clock. An end-to-end transparent clock measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an follow-up message. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.7.0S/ASR903-Chassis-SW-37.html.
- GOLD—Generic Online Diagnostic (GOLD) is a health monitoring feature implemented on the Cisco ASR 903 Router. The GOLD functionality is developed to provide online diagnostic capabilities that run at bootup, in the background on a periodic basis, or based on demand from the CLI. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/GOLD.html.
- Hot Standby Pseudowire Support—The Hot Standby Pseudowire feature provides faster failover of a backup pseudowire and reduced traffic loss during failover by setting the backup pseudowire to a hot standby state, such that it can immediately take over if the primary pseudowire fails. This feature is supported for Ethernet only; TDM and ATM interfaces are not supported. For more information, see:
  - http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap6.html.

  - http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fspseudo.html
  - http://www.cisco.com/en/US/partner/docs/ios/mpls/configuration/guide/mp_hspw_for_atm.html#wp1054150

- Hybrid Clocking Support—Hybrid clocking mode that uses clock frequency obtained from the synchronous Ethernet port while using phase (ToD or 1PPS) obtained using PTP. The combination of multiple time and phase sources for the same master clock improves performance over using PTP alone. The router can act as a hybrid clock in both master ordinary clock and slave ordinary clock. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.7.0S/ASR903-Chassis-SW-37.html.
- IPv6 ACL—IPv6 Access Control Lists (ACLs) determine what traffic is blocked and what traffic is forwarded at device interfaces. ACLs allow filtering based on source and destination addresses, inbound and outbound to a specific interface. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/IPv6_ACL.html.
- Layer 2 QoS for ATM—This feature introduces support for support cbr and vbr on ATM interfaces. For more information, see http://www.cisco.com/en/US/partner/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-3s/qos-atm-vp-support-xe.html
- Link Path Through—This feature enables a local EoMPLS PE router to detect a failure in the path between the remote PE and CE routers. The local PE router propagates the failure to the local CE router such that it brings down the pseudowire connection and can more quickly reestablish the connection when the remote CE-PE connection is restored. This feature is enabled automatically and does not introduce any new CLI commands.
- MAC Address Security for EVC Bridge-Domain—MAC address security for EVCs. Provides the capability to control and filter the MAC address learning behavior at the granularity of a single EVC service instance. For more information, see:
  - http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-mac-addlmt-bdsin.html
  - http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/ce-mac-addlmt-bdsin.html
- MAC Limiting—Mac address limiting per bridge-domain restricts the number of MAC addresses that the router learns in bridge-domain on an EFP, pseudowire or switch port. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/mac_limiting.html.
- MPLS VPN—The MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses feature allows a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) to span service providers and autonomous systems. For more information, see http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_connect_asbr.html.
- Multicast Static MAC Addresses— Static MAC addresses allow you to enable multicast at the layer 2 level. You can use multicast static MAC addresses to forward multicast packets to specific EFPs on a network. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/evc.html.
- Multi-Level Priority Queues (MPQ)—This feature allows you to configure multiple priority queues for multiple traffic classes by specifying a different priority level for each of the traffic classes in a single service policy map. You can configure multiple service policy maps per router. Having multiple priority queues enables the router to place delay-sensitive traffic (for example, voice) on the outbound link before delay-insensitive traffic. As a result, high-priority traffic receives the lowest latency possible on the router. For more information, see:

  - http://www.cisco.com/en/US/docs/ios-xml/ios/qos_conmgt/configuration/xe-3s/asr903/qos-conmgt-multilevel-pq.html
  - http://www.cisco.com/en/US/docs/ios-xml/ios/qos_conmgt/configuration/xe-3s/qos-conmgt-multilevel-pq.html

- N:1 PVC mapping to PWE with non-unique VPI—This feature allows you to map one or more ATM permanent virtual circuits (PVCs) to a single pseudowire. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/atm/configuration/15-2s/atm-n1pvc-mapping.html.
- Onboard Failure Logging—The Onboard Failure Logging (OBFL) feature collects data such as operating temperatures, hardware uptime, interrupts, and other important events and messages from system hardware installed in a Cisco router or switch. The data is stored in nonvolatile memory and helps technical personnel diagnose hardware problems. For more information, see http://www.cisco.com/en/US/docs/wireless/asr_900/feature/guides/onboard_failure_logging.html.
- PTP Redundancy—PTP redundancy allows a PTP slave clock to select the best master from multiple available master clocks based on clock quality and availability. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.7.0S/ASR903-Chassis-SW-37.html.
- Time of Day Selection—You can use the time of day (ToD) and 1PPS ports on the Cisco ASR 903 Series Router to exchange ToD clocking. In master mode, the router can receive time of day (ToD) clocking from an external GPS unit; the router requires a ToD, 1PPS, and 10Mhz connection to the GPS unit. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.7.0S/ASR903-Chassis-SW-37.html

4

New Features in Cisco IOS XE 3.8S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE Release 3.8S.

This chapter includes the following sections:

New HardwareFeatures in Cisco IOS XE Release 3.8(2)S

The IOS XE 3.8(2)S Release for the Cisco ASR 903 Router does not introduce any new hardware features.

New Hardware Features in Cisco IOS XE Release 3.8(1)S

The IOS XE 3.8(1)S Release for the Cisco ASR 903 Router does not introduce any new hardware features.

New Hardware Features in Cisco IOS XE Release 3.8(0)S

The IOS XE 3.8(0)S Release for the Cisco ASR 903 Router introduces the following hardware features:

Release 3.8(0)S introduces support for the following SFPs:

- GLC-FE-100BX-U
- GLC-FE-100BX-D
- GLC-FE-100LX

- GLC-FE-100FX
- ONS-XC-10G-EP30.33
- XFP10GER-192IR-L
- XFP10GLR-192SR-L
- XFP-10GZR-OC192LR

For more information about how to configure these SFPs, see:
http://www.cisco.com/en/US/partner/docs/interfaces_modules/transceiver_modules/installation/note/OL_24246.html

http://www.cisco.com/en/US/partner/products/hw/modules/ps5455/tsd_products_support_series_home.html

New SoftwareFeatures in Cisco IOS XE Release 3.8(2)S

The IOS XE 3.8(2)S Release for the Cisco ASR 903 Router does not introduce any new software features.

New Software Features in Cisco IOS XE Release 3.8(1)S

Release 3.8(1) introduces support for the following software features:

- uRPF Loose Mode—This release introduces support for Unicast Reverse Path Forwarding (uRPF) Loose mode. For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_urpf/configuration/xe-3s/sec-unicast-rpf-loose-mode.html

New Software Features in Cisco IOS XE Release 3.8(0)S

Release 3.8(0) introduces support for the following software features:

- Automatic Protection Switching—This release introduces support for Automatic protection switching (APS) for link failure protection on SONET networks. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/feature/guide/APS.html
- ATM IMA on OC-3 Interfaces—This release introduces support for ATM IMA on the OC-3 interface module. For more information about this feature, see the *Cisco ASR 903 Router Chassis Configuration Guide, Release 3.8*.
- BFD Support on TDM interfaces—Release 3.8 introduces support for BFD on TDM interfaces. This feature does not introduce any new CLI.
- BFD Support for HSRP—This release extends Bidirectional Forwarding Detection support in order to send failure notifications using the Hot Standby Router Protocol (HSRP). For more information about this feature, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html
- BFD Timer Improvements—Release 3.8 introduces support for 3.3ms timers for offloaded IPv4 BFD traffic.

- BGP PIC—This release introduces support for BGP Prefix-Independent Convergence (PIC). This feature improves BGP convergence after a network failure. This convergence is applicable to both core and edge failures and can be used in both IP and MPLS networks. The BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB), and Cisco Express Forwarding so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover. For more information, see http://www.cisco.com/en/US/partner/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/asr903/irg-xe-3s-asr903-book.html
- VPLS BGP Signaling—This release introduces support for VPLS BGP Signaling. The two primary functions of the Virtual Private LAN Service (VPLS) control plane are autodiscovery and signaling. The VPLS BGP Signaling feature enables you to use BGP as both an autodiscovery and a signaling protocol for VPLS. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/asr903/irg-vpls-bgp-sig.html
- E-LMI PE Support—This release introduces support for Ethernet Local Management Interface (LMI) at the Provider Edge (PE). For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-elmi-pe.html
- IP SLA Y.1731 SLM Feature Enhancements—This release introduces support for IP SLA SLM enhancements as described in the Y.1731 standard. For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3s/asr903/sla_y1731_demand.html
- IS-IS Support for BFD over IPv6—This release introduces support for BFD on IS-IS IPv6 connections. For more information about this feature, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html
- LACP Min-Links—This release introduces support for Etherchannel Min-Links, a minimum threshold for the number of links in an Etherchannel before the it becomes active. For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-ieee-link-bndl-xe.html
- Microwave Adaptive Bandwidth—This release introduces support for Microwave Adaptive Bandwidth with G.8032 and CFM. For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-cfm-adapt-bandwidth.html
- MPLS on PoS Interfaces—Release 3.8 introduces support for MPLS on Packet over SONET (PoS) interfaces. For more information about this feature, see the *Cisco ASR 903 Router Chassis Configuration Guide, Release 3.8*.
- MPLS-TP MIB—This release introduces support for the MPLS-TP MIB. For more information about using MIBs, see MIB Support, page 4.
- MPLS-TP Pseudowire Support—This release introduces support for MPLS-TP on ATM and TDM pseudowires. For more information, see the *Cisco ASR 903 Router Chassis Configuration Guide, Release 3.8* and http://www.cisco.com/en/US/docs/ios-xml/ios/mp_basic/configuration/xe-3s/mp-mpls-tp.html
- OC-3 MLPPP QoS Support—Release 3.8 introduces support for QoS policies on egress MLPPP interfaces on the optical interface module.

- Multicast on T1/E1 and Optical Interfaces—Release 3.8 introduces support for multicast on T1/E1 and OC-3 interface modules. For more information about multicast, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html.
- Network Virtualization Service—This Release introduces support for the Satellite Network Virtualization (nV) service or the Satellite Switching System, which enables you to configure a topology in which satellite devices complement one or more Cisco ASR 9000 Series routers in order to collectively realize a single virtual switching system. In this system, the satellite switches act under the management control of the Cisco ASR 9000 Series Aggregation Services Routers. The complete configuration and management of the satellite chassis and features is performed through the control plane and management plane of the Cisco ASR 9000 Series Router. For more information about how to configure nV on the ASR 9000 and the satellite devices, see http://www.cisco.com/en/US/partner/docs/routers/asr9000/software/asr9k_r4.2/interfaces/configuration/guide/hc42satl.html
- Packet over SONET—This release introduces support for Packet over SONET (PoS) interfaces on the OC-3 interface module. For more information on how to configure PoS interfaces, see the *Cisco ASR 903 Chassis Configuration Guide, Release 3.8*.
- QoS on PoS Interfaces—Release 3.8 introduces support for QoS features on egress PoS interfaces using MLPPP bundles. For more information about configuring QoS on MLPPP interfaces, see the *Cisco ASR 903 Chassis Configuration Guide, Release 3.8.*
- QoS Features—Release 3.8 introduces support for the following QoS features:
  - **queue-limit percent** command— Allows you to specify the queue limit (size) for a class in as a percentage value.
  - Higher Queue Limit Size— Release 3.8 extends the maximum byte value *queue-limit-size* argument used with the **queue-limit** command. The previous maximum value was 491520 bytes; the new value is 2 MB.
  - Release 3.8 enhances the **show policy-map interface** command to display the default queue-limit.

  For more information about the Release 3.8 QoS features, see the QoS chapter of the *Cisco ASR 903 Chassis Configuration Guide, Release 3.8.*
- SONET Mode—This release introduces support for SONET mode on the OC-3 interface module. For more information on how to configure PoS interfaces, see the *Cisco ASR 903 Chassis Configuration Guide, Release 3.8*.
- Synthetic Frame Loss Measurement—This release introduces support for Synthetic Frame Loss Measurement for Ethernet OAM. For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3s/asr903/sla_mether3_y1731.html
- TCP path MTU Support—This release introduces support for BGP TCP Path MTU Discovery. For more information about this feature, see http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html
- Telecom Profile Support—Release 3.8 introduces support for telecom profiles, which allow you to configure a network clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. For information about how to configure telecom profiles, see the *Cisco ASR 903 Chassis Configuration Guide, Release 3.8.*
- Trunk EFPs on Port-Channel Interfaces—This release adds support for trunk EFPs on port-channel interfaces, as shown in the following configuration:

```
!
```

```
interface port-channel 4
 service instance 1 ethernet
  encapsulation untagged
  l2protocol peer lacp
  bridge-domain 1
 !
 service instance trunk 10 ethernet
  encapsulation dot1q <>
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
!
```

For more information about configuring EFP interfaces, see the Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.

- Y.1731 enhancements—This release introduces support for Y.1731 on-demand and concurrent features. For more information about this feature, see http://www.cisco.com/en/US/partner/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-y1731-perfmon.html

5

New Features in Cisco IOS XE 3.9S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE Release 3.9S and includes the following sections:

New Hardware Features in Cisco IOS XE Release 3.9(2)S

There are no new hardware features introduced in Cisco IOS XE Release 3.9(2)S.

New Software Features in Cisco IOS XE Release 3.9(2)S

There are no new software features introduced in Cisco IOS XE Release 3.9(2)S.

New Hardware Features in Cisco IOS XE Release 3.9(1a)S

Release 3.9(1) introduces support for the following hardware features:

- GLC-FE-100EX
- GLC-FE-100ZX
- SFP-GE-L
- SFP-GE-S
- SFP-GE-Z

New Software Features in Cisco IOS XE Release 3.9(1a)S

There are no new software features introduced in Cisco IOS XE Release 3.9(1)S.

New Hardware Features in Cisco IOS XE Release 3.9(0)S

Release 3.9(0) introduces support for the following hardware features:

- DWDM-XFP-30.33
- DWDM-XFP-31.12
- DWDM-XFP-31.90
- DWDM-XFP-32.68
- DWDM-XFP-34.25
- DWDM-XFP-35.04
- DWDM-XFP-35.82
- DWDM-XFP-36.61
- DWDM-XFP-38.19
- DWDM-XFP-38.98v
- DWDM-XFP-39.77
- DWDM-XFP-40.56
- DWDM-XFP-42.14
- DWDM-XFP-42.94
- DWDM-XFP-43.73
- DWDM-XFP-44.53
- DWDM-XFP-46.12
- DWDM-XFP-46.92
- DWDM-XFP-47.72
- DWDM-XFP-48.51
- DWDM-XFP-50.12
- DWDM-XFP-50.92
- DWDM-XFP-51.72v
- DWDM-XFP-52.52
- DWDM-XFP-54.13
- DWDM-XFP-54.94
- DWDM-XFP-55.75
- DWDM-XFP-56.55
- DWDM-XFP-58.17
- DWDM-XFP-58.98
- DWDM-XFP-59.79

- DWDM-XFP-60.61
- DWDM-XFP-C
- DWDM-XFP-1560.61

New Software Features in Cisco IOS XE Release 3.9(0)S

Release 3.9(0) introduces support for the following software features:

- BFD Echo Mode Hardware Offloading—BFD echo mode detects forwarding path failures on the remote system using echo packets; this release introduces support for hardware offloading of BFD echo mode packets for up to 255 sessions. The minimum supported timer value for offloaded BFD echo mode sessions is 3.3 ms. BFD echo offloading directs BFD echo packets to the high priority queue instead of the default queue. For more information about how to configure BFD, see IP Routing: BFD Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 903).
- BGP Support for 4-byte ASN —This release introduces support for 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/asr903/irg-4byte-asn.html
- CFM Support for Trunk EFP—This release introduces support for CFM on trunk EFP interfaces. For more information about configuring EFPs, see *Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router*. For more information about configuring CFM, see the *Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S (ASR 903).*
- Enhanced Object Tracking—The Enhanced Object Tracking feature separates the tracking mechanism from Hot Standby Router Protocol (HSRP) in order to create a separate standalone tracking process. The tracking process is available to other IOS processes and allows tracking of other objects in addition to the interface line-protocol state. For more information, see http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_eot_xe.html.
- Embedded Event Manager (EEM) 4.0—Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/eem/configuration/xe-3s/eem-overview.html.
- IP FRR/Remote LFA FRR with L2VPN—The Loop-Free Alternate (LFA) Fast Reroute (FRR) with Layer 2 Virtual Private Network (L2VPN) feature minimizes packet loss due to link or node failure. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-3s/asr903/mp-l2vpn-lfa-frr.html.
- IS-IS topology of 3000 nodes—This release extends IS-IS capacity to include support for 3000 nodes. For more information about configuring IS-IS routing, see *IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 903)*.
- ISO OSI Routing—This release introduces support for ISO OSI routing.
- Link Layer Discovery Protocol—Link Layer Discovery Protocol (LLDP) is defined in the IEEE 802.1ab standard and allows a non-Cisco device to interact with a Cisco device that uses Cisco Discovery Protocol (CDP) for topology discovery. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-lldp-multivend.html.

- L2VPN Protocol Support—This release introduces support for additional L2VPN protocols including L2TP and UDP. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-3s/l2vpn-prot-based.html
- Microwave Adaptive Bandwidth Modulation Enhancement—This release introduces support for Adaptive Bandwidth Modulation on G.8032 and E-OAM microwave connections, which allow Ethernet switches to optimize traffic forwarding rules based on microwave link capacity. For more information, see
  - http://www.cisco.com/en/US/docs/routers/asr903/feature/guide/mw_acm.html
  - http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/xe-3s/asr903/ce-cfm-adapt-bandwidth.html.
- MPLS on MLPPP Interfaces—This release introduces support for MPLS on MLPPP interfaces. For more information about configuring MPLS, see the *MPLS Basic MPLS Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 903)*. For more information about configuring MLPPP interfaces, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html.
- MPLS -TP Linear Protection/PSC support—Linear Protection on MPLS-TP based transport networks using the RFC 6378 standard. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/mp_basic/configuration/xe-3s/asr903/mp-basic-xe-3s-asr903-book.html.
- MVPN—The Multicast VPN (MVPN) feature provides the ability to support multicast over a Layer 3 Virtual Private Network (VPN). For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_mvpn/configuration/xe-3s/asr903/imc_cfg_mc_vpn.html.
- On-Demand Y.1731PM Probe Execution—This release introduces support for IPSLA Y1731 SLM enhancements that enable real-time Ethernet service troubleshooting for users without configuration privileges. This feature supports on-demand Synthetic Loss Measurement (SLM) operations that can be run by issuing a single command in privileged EXEC mode. For more information, see http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/xe-3s/sla_y1731_demand.html
- OC-12 HDLC, PPP, and MLPPP support—This release introduces support for HDLC, PPP, and MLPPP on OC-12 interfaces. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html.
- POS (Packet over SONET/SDH) on OC12 IM card—This release introduces support for Packet over SONET (POS) and SDH on OC-12 interfaces. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html
- PTP over Native Ethernet—This release introduces support for IEEE 1588-2008 Precision Time Protocol (PTP) on native Ethernet interfaces; this allows the router to deliver the PTP payload within an Ethernet packet. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html.
- QoS Ingress Exp Bit Marking—This release introduces support for ingress QoS marking of MPLS Exp bits on TDM and ATM pseudowires. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html.

- QoS Match on EFP—This release introduces support for QoS matching on EFP interfaces. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html.
- QoS on OC-3 and OC-12 Interfaces—This release introduces support for two-level QoS policies on OC-3/OC-12 serial, MLPPP, and PoS interfaces. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html.
- QoS Support for Ether Channels—This release introduces support for QoS policies on Etherchannel interfaces. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html.

New Features in Cisco IOS XE 3.10S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE Release 3.10S.

This chapter includes the following sections:

New Hardware Features in Cisco IOS XE Release 3.10.2S

There are no new hardware features introduced for Cisco IOS XE Release 3.10.2.S.

New Hardware Features in Cisco IOS XE Release 3.10.1S

The IOS XE 3.10S Release for the Cisco ASR 903 Router introduces the following hardware features:

DC PEM Module (A900-PWR550-D-E)

The power supply provides 550 W output power for system 12 V power. The power supply is field replaceable, hot-swappable, and operates separately from the fan tray. The power supply contains a front panel with mounting screws, a handle for insertion and removal, and two status LEDs. No ON/OFF switch is provided

The A900-PWR550-D-E DC PEM module has a T-shaped power input terminal connector. For information on DC PEM module specifications, see Cisco ASR 903 router Overview. For information on installing the connector, see Installing the Cisco ASR 903 Series Aggregation Services Router.

Fan Tray (A903-FAN-E)

The A903-FAN-E is a fan tray containing twelve (40 x 40 x 20 mm) fans and provides sufficient capacity to maintain operation indefinitely in the event of an individual fan failure. For information on installing the fan tray, see Installing the Cisco ASR 903 Series Aggregation Services Router.

Dust Filter (A903-FAN-F)

The dust filter on the fan tray is a quadrafoam 45PPI filter which is 85 percent dust resistant. For information on installing the dust filter, see Installing the Cisco ASR 903 Series Aggregation Services Router.

Dummy Cover (A903-FAN-F-B)

A dummy cover (A903-FAN-F-B) secures the dust filter in the chassis. For installing the fan filter, see For information on installing the dummy cover on the fan tray, see Installing the Cisco ASR 903 Series Aggregation Services Router.

Cable Bracket (A903-CAB-BRACKET)

The cable management bracket helps in routing the cables from the interface modules; therefore enabling a proper cable bending radius. For installing the bracket, see Installing the Cisco ASR 903 Series Aggregation Services Router.

Air Plenum

Air Plenum or air baffle assembly is used change the air flow pattern of the unit. When the router is installed with the plenum, the air flow pattern is changed from side-side to front-back. For information on ordering the air plenum, see Installing the Cisco ASR 903 Series Aggregation Services Router.

New Hardware Features in Cisco IOS XE Release 3.10S

The IOS XE 3.10S Release for the Cisco ASR 903 Router introduces the following hardware features:

Serial Interface Module

IOS XE Release 3.10(0)S introduces support for the serial interface module, which is designed to provide a low-latency communication platform for legacy interfaces. Designed for utilities, the module is hardened to accommodate the wide operating temperature swings, EMI and surge spikes, and dust found in substation environments.

The combination of the Cisco ASR 903 Router and the serial interface module enables migration from TDM and serial networks to an IP-based network that can control latency and jitter across the network and enable multiple Smart Grid applications.

The Cisco ASR 903 Serial Interface Module supports the following standards:

- EEE 1613 2009—IEEE Standard for Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations
- EC 61850-3—IEC standard specifying general requirements for substation automation systems (SAS) communications and related system requirements.
- EC 60870-2-1:1995—IEC standard for substation environmental conditions
- EC 60870-2-2:1996—IEC standard for substation environmental conditions
- EC 61000-6-5:2001—IEC standard defining immunity for power station and substation environments

For information on how to install the serial interface module, see the *Cisco ASR 903 Hardware Installation Guide*.

For information on how to configure the serial interface module, see *Configuring Raw Socket Transport on the Cisco ASR 903 Router.*

Note We recommend the installation of the Metro IP Services and Metro Aggregation Services licenses with serial interface module. For more information about obtaining and installing licenses, see Software Licensing Overview.

CWDM SFP

Cisco IOS XE Release 3.10S introduces support for the following SFPs on the 10 Gigabit Ethernet XFP Interface Module:

- ONS-XC-10G-EP
- ONS-XC-10G-1470
- ONS-XC-10G-1490
- ONS-XC-10G-1510
- ONS-XC-10G-1530
- ONS-XC-10G-1550
- ONS-XC-10G-1570
- ONS-XC-10G-1590
- ONS-XC-10G-1610

For more information about how to configure these SFPs, see:
http://www.cisco.com/en/US/partner/docs/interfaces_modules/transceiver_modules/installation/note/OL_24246.html

http://www.cisco.com/en/US/partner/products/hw/modules/ps5455/tsd_products_support_series_home.html

New Software Features in Cisco IOS XE Release 3.10.2S

There are no new software features introduced for Cisco IOS XE Release 3.10.2.S.

New Software Features in Cisco IOS XE Release 3.10.1S

There are no new software features introduced for Cisco IOS XE Release 3.10.1.S.

New Software Features in Cisco IOS XE Release 3.10S

The following features are introduced in Cisco IOS Release 3.10S.

Access Circuit Redundancy

Access Circuit Redundancy (ACR) enables local switching for circuit emulation (CEM) interfaces by creating a virtual CEM-ACR interface. All configuration changes made on the virtual CEM-ACR interface are applied automatically on both the Working and Protect interfaces.

For more information see, *Configuring Access Circuit Redundancy on the Cisco ASR 903 Router*.

Access Switch Device Manager Template

The Switch Device Manager (SDM) templates are used to optimize system resources in the router to support specific features, depending on how the router is used in the network. The SDM templates allocate Ternary Content Addressable Memory (TCAM) resources to support different features.

Note SDM templates are supported only by the Metro Aggregation Services license.

For more information see, *Configuring Access Switch Device Manager Template on the Cisco ASR 903 Router.*

Auto-IP

The Auto-IP feature addresses the problem of manually reconfiguring nodes during insertion, deletion, and movement of nodes within an auto-IP ring. The auto-IP feature automatically provides IP addresses to the node interfaces inserted into an auto-IP ring.

For more information, see *Auto-IP*.

BFD Debug Enhancement

The Bidirectional Forwarding Detection (BFD) Debug Enhancement feature enhances the BFD debug messages and the show command output and enables logs and history for critical BFD events. This feature helps network engineers and operators to easily identify any issues with BFD sessions or events.

The following commands were introduced for this feature: monitor event-trace bfd, monitor event-trace bfd event, monitor event-trace bfd packet, and show monitor event-trace bfd.

For more information, refer to the *IP Routing: BFD Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 903)*, *IP Routing Protocol-Independent Commands A through R*, and *IP Routing Protocol-Independent Commands S through T*.

Bidirectional Forwarding Detection Deterministic Hardware Offload

The Bidirectional Forwarding Detection (BFD) deterministic hardware offload feature allows you to define the BFD transmission timer value. Any BFD sessions below or equal to the set value are sent to hardware.

For more information see, *Bidirectional Forwarding Detection Deterministic Hardware Offload.*

Broadcast and Multicast Suppression

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic broadcast and multicast suppression (or storm control) feature prevents LAN ports from being disrupted by a broadcast, multicast and unicast traffic storm on physical interfaces.

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. Storm control is applicable for physical interfaces and is used to restrict the unicast, broadcast and multicast ingress traffic on the Layer2 interfaces. The feature is disabled by default on the Cisco ASR 903 router.

For more information see, *Configuring Broadcast and Multicast Suppression on the Cisco ASR Router.*

IGMP Snooping

IP Multicast Internet Group Management Protocol (IGMP), which runs at Layer 3 on a multicast device, generates Layer 3 IGMP queries in subnets where the multicast traffic must be routed. IGMP (on a device) sends out periodic general IGMP queries.

IGMP Snooping is an Ethernet Virtual Circuit (EVC)-based feature set. When IGMP snooping is enabled on a bridge domain, the bridge domain interface responds at Layer 2 to the IGMP queries with only one IGMP join request per Layer 2 multicast group. Each bridge domain represents a Layer 2 broadcast domain.

For more information see, *Configuring IGMP Snooping on Cisco ASR 903 Router*.

Licensing the OC-3 and OC-12 Interface Modules

The optical modules 4-Port OC3/STM-1 or 1-Port OC12/STM-4 delivers four active ports of OC-3 interface module (IM) or Synchronous Transport Module level 1 (STM-1) connectivity, or one active port of OC-12 IM or STM-4 connectivity, on the Cisco ASR 903 Router. Licensing is applicable to these ports on the interface modules.

The benefits of licensing these ports are:

- Facilitate the pay-as-you-grow model to enhance the ports by purchasing licenses as required.
- Provide the ability to shift license from one port to another.
- Provide the ability to release a license when the interface module is removed from a slot and reinstall the license when inserted again.
- Support for high availability and OIR of interface modules.

Table 6-1 lists the license supported on the OC-3 and OC-12 interface modules.

Table 6-1 OC-3 and OC-12 Port Licenses

License Type	Description	Usability
1 OC3 port license	Single OC3/STM-1 port	STM-1 on OC-3 port
1 OC12 port license	Single OC12/STM-4 port	STM-1 on OC-3 port

For more information see, *Licensing the OC-3 and OC-12 Interface Modules on the Cisco ASR 903 Router*.

Multichassis LACP

Cisco's Multichassis EtherChannel (MCEC) solution addresses the need for interchassis redundancy mechanisms, where a carrier wants to "dual home" a device to two upstream points of attachment (PoAs) for redundancy. Some carriers either cannot or will not run loop prevention control protocols in their access networks, making an alternative redundancy scheme necessary. MCEC addresses this issue with enhancements to the 802.3ad Link Aggregation Control Protocol (LACP) implementation. These enhancements are provided in the Multichassis LACP (mLACP) feature.

For more information, see *Multichassis LACP*.

Pseudowire Group Switchover

Currently, pseudowire switchovers to the backup pseudowires occur one by one from IOS to platform dataplane and can take up to four seconds for 1000 pseudowires. The group switchover feature reduces this switchover time by efficiently grouping status messages in both Label Distribution Protocol (LDP) and internal Inter-Process Communications (IPCs).

Note The Pseudowire Group Switchover feature is enabled by default and cannot be disabled.

For more information, see *Cisco ASR 903 Router Chassis Software Configuration Guide, IOS XE Release 3.10S*.

Raw Socket

Raw Socket Transport is a method for transporting serial data through an IP network. Raw Socket transports Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). This method is an alternative to the Block Serial Tunnel (BSTUN) protocol. Raw Socket supports point-to-point and point-to-multipoint connections. For instructions on how to configure Raw Socket, see Configuring Raw Socket Transport on the Cisco ASR 903 Router.

Raw Socket is supported on the serial interface module. For instructions on how to install the serial interface module, see the Cisco ASR 903 Hardware Installation Guide.

For information on how to configure the serial interface module, see *Configuring Raw Socket Transport on the Cisco ASR 903 Router.*

Note We recommend the installation of the Metro IP Services and Metro Aggregation Services licenses with serial interface module. For more information about obtaining and installing licenses, see *Software Licensing Overview*.

Hardware Limitations

Serial Interface Module Limitations—The following limitations apply to the serial interface module:

- A maximum of 2 serial interface modules are supported on the Cisco ASR 903 Router.
- The serial interface module hardware supports a 230.4 Kbps traffic rate in asynchronous mode. The actual speed is dependent on cable quality and length. The serial interface module hardware supports an 8 Mbps traffic rate in synchronous mode. The actual speed is dependent on cable quality and length.

Software Limitations

Raw Socket limitations—The following software limitations apply to the serial interface module:

- Raw Socket encapsulation is supported on up to 28 serial ports.
- Asynchronous EIA/TIA-232 serial traffic is supported with DB-25, DB-9, and RJ-45 connectors.
- The X.21, V.35, RS-485, EIA-449, EIA-530, and IRIG-B standards are not currently supported by software.
- Synchronous traffic is not currently supported.

Remote LFA FRR Protection for TDM and ATM Pseudowires

Starting with Cisco IOS XE Release 3.10S, the Loop-Free Alternate (LFA) Fast Reroute (FRR) feature is supported for Time-division multiplexing (TDM) pseudowires.

- Circuit Emulation Service over Packet Switched Network (CESoPSN) over MPLS, and Structure-Agnostic Time Division Multiplexing over Packet (SAToP) over MPLS networks for T1, E1, SDH and SONET framing is supported.
- Inverse Multiplexing over ATM (IMA) over MPLS; PVC and PVC sessions are supported for the ATM (IMA).

For more information see, *Configuring Loop-Free Alternate Fast Reroute on the Cisco ASR 903 Router*.

Remote LFA FRR and Labeled BGP PIC FRR Integration

Starting with Cisco IOS XE Release 3.10S, Both the Labeled Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC) feature and the Loop-Free Alternate (LFA) Fast Reroute (FRR) feature can be configured together on the Cisco ASR 903 router.

For more information see, *Configuring Loop-Free Alternate Fast Reroute on the Cisco ASR 903 Router*.

VPLS over Remote LFA

Starting with Cisco IOS XE Release 3.10, Virtual Private LAN Services (VPLS) is supported on the Cisco ASR 903 router.

For more information see, *Configuring Loop-Free Alternate Fast Reroute on the Cisco ASR 903 Router*.

New Features in Cisco IOS XE 3.11S Releases

This chapter provides information about the new features introduced in the Cisco IOS XE Release 3.11S.

This chapter includes the following sections:

New Hardware Features in Cisco IOS XE Release 3.11S

There are no new hardware features for Cisco IOS XE Release 3.11 S.

New Software Features in Cisco IOS XE Release 3.11S

The following features are introduced in Cisco IOS Release 3.11S.

AAL5 termination

This feature enables the Asynchronous Transfer Mode Adaptation Layer 5 (AAL5) layer 3 termination on the interface module (IM) (T1/E1 and OC-3) cards on the Cisco ASR 903 Router.

For more information see,
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_Configuring_AAL5_termination_903.html

Access Switch Device Manager Template

This feature can be used to configure system resources on the router to optimize support for specific features, depending on how the router is used in the network.

For more information see,
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_SDM_ASR903.html

Data Plane Ethernet Loopback with QoS

The Ethernet data plane loopback feature provides a means for remotely testing the throughput of an Ethernet port. For more information see,
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_layer2_ASR903_chapter_00.html.

Dissimilar PHB Match at Ingress and Egress

The dissimilar per-hop behavior (PHB) **match** on exp is supported for Ingress and Egress on MPLS and VPLS interfaces.

In earlier releases prior to Cisco IOS XE Release 3.11S, when **qos-group** or **discard-class** based on exp classification was configured, Egress based classification was *not* allowed on any other classification except Ingress **set qos-group** or **discard-class**. This was due to the PHB security model.

With Cisco IOS Release 3.11, only EVC based tunnel type configuration with either Layer2 VPN or Layer3 VPN is supported.

For more information see,
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_QoS_guidelines_903_chapter_00.html

Dying Gasp

This feature generates an alert when the Cisco ASR 903 Router encounters any of the following conditions:

- Interface error-disable
- Reload
- Power failure or removal of power supply cable

For more information see,
http://www.cisco.com/en/US/docs/routers/asr903/feature/guide/Dying_Gasp_ASR_903.html.

DS3 Framing on OC-3 and OC-12

This feature introduces support for the DS3 clear channel for OC-3 and OC-12 interface modules. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/OC_Ifc_Module.html.

Fast Reroute Support for Bridge Domain Interface

Fast Reroute is supported on bridge domain interfaces on the Cisco ASR 903 router. For more information, see http://www.cisco.com/en/US/docs/routers/asr903/feature/guide/b_lfa_frr_903.html.

BGP PIC Support for Bridge Domain Interface with FRR

BGP PIC is supported on bridge domain interfaces with FRR on the Cisco ASR 903 router. For more information on configuring BGP PIC, see http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/asr903/irg-bgp-mp-pic.html.

IPv6 Multicast: Multicast Listener Discovery (MLD)

This feature is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links.

For more information see, http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_ipmcast_pim_xe_3S_asr903_chapter_0101.html

IPv6 Multicast: PIM v6

This feature supports the following:

- PIM Source-Specific Multicast—The PIM source-specific multicast (SSM) routing protocol supports SSM implementation and is derived from PIM-SM.
- PIM Sparse Mode (PIM-SM)—IPv6 multicast provides support for intra domain multicast routing using PIM sparse mode (PIM-SM).
- PIM Embedded RP Support—Embedded RP support allows the device to learn RP information using the multicast group destination address instead of the statically configured RP.
- PIM Accept Register—supports the PIM accept register feature to perform PIM-SM register message filtering at the RP.

For more information see, http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_ipmcast_pim_xe_3S_asr903_chapter_0110.html

ISIS and OSPF Local Microloop Protection

For ISIS Micoloop Protection, see
http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/xe-3s/irs-uloop-local-avoid.html

For OSPF Microloop Protections, see
http://www.cisco.com/en/US/partner/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-ospfv2-ip-frr.html

MR-APS Integration with Hotstandby Pseudowire

This feature is a protection mechanism for Synchronous Optical Network (SONET) networks that enablesSONET connections to switch to another SONET circuit when a circuit failure occurs.For more information see,
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_MR_APS_ASR903.html

Remote SPAN

This feature is used for remote monitoring of multiple devices at source port, source Vlan levels in the Layer2 network. For more information, see
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_layer2_ASR903_chapter_01.html

Service Groups

The Service groups feature allows you to create service groups and apply aggregate features to those service groups.

For more information, see
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_QoS_guidelines_903_chapter_00.html

TCAM Threshold Based Alarms

This feature generates syslog and consequently a Simple Network Management Protocol (SNMP) trap when an application reaches the preset threshold for its allotted TCAM size.

For more information, see
http://www.cisco.com/en/US/docs/routers/asr903/software/guide/b_TCAM_alarms_ASR903.html.

Restrictions and Caveats in Cisco IOS XE 3.6S Releases

This chapter provides information about restrictions and caveats in Cisco IOS XE 3.6S releases.

Note Because Cisco IOS XE 36S is based on Cisco IOS XE 3.5 inherited releases, some caveats that apply to Cisco IOS XE 3.5 releases also apply to Cisco IOS XE 36S. Release 3.5 is not described in this document; for a list of the software caveats that apply to Cisco IOS XE 3.5, see the Release Notes for Cisco IOS XE Release 3S.

Note We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

This chapter contains the following sections:

Limitations and Restrictions

The following sections describe the Cisco ASR 903 Router limitations:

Limitations and Restrictions in Cisco IOS XE Release 3.6(2)S

Note For a summary of limitations in Release 3.5S, see the IOS XE 3.5 Release Notes.

The following limitations apply to the Cisco ASR 903 Router in IOS XE Release 3.6(2)S:

- SAToP and CESoPSN pseudowire traffic has a default MPLS Exp priority setting of 5 (high).

The limitations for this release are otherwise the same as those for IOS XE Release 3.6(2)S. For more information, see the Limitations and Restrictions in Cisco IOS XE Release 3.6(1)S, page 2.

Limitations and Restrictions in Cisco IOS XE Release 3.6(1)S

The following limitations apply to the Cisco ASR 903 Router in IOS XE Release 3.6(1)S:

Note For a summary of limitations in Release 3.5S, see the IOS XE 3.5 Release Notes.

ATM IMA Limitation

- You can create a maximum of 16 IMA groups on each T1/E1 interface module.

Bridge Domain Interface Limitation

- The **mtu** command is not supported on BDI interfaces; however the **ip mtu** command is supported.

Clocking and Timing Limitation

- Only a single clocking input source can be configured within each group of eight ports (0-7 and 8-15) on the T1/E1 interface module using the network-clock input-source command.

EFP Limitation

- QinQ is not supported on trunk EFP interfaces.

Ethernet IM Limitations

- The Cisco ASR 903 Router does not support the Facilities Data Link (FDL) on Ethernet interfaces.
- The Cisco ASR 903 Router does not support the **mac-address** command on Gigabit Ethernet interface modules.
- 10 Gigabit Ethernet interface modules are not supported in slots 4 and 5.

When you install a Gigabit Ethernet IM in the topmost interface module slot (slot 5), the last interface (interface GigabitEthernet0/5/0) is not operational; the port is reserved for internal communication.

MLPPP Limitations

The following limitations apply when using MLPPP in IOS XE Release 3.6 on the Cisco ASR 903 Router:

- All links in an MLPPP bundle must be on the same interface module.
- All links in an MLPPP bundle must be of the same bandwidth.
- The Cisco ASR 903 Router supports a maximum of 8 links per bundle
- To change the MLPPP bundle fragmentation mode between enabled and disabled, perform a **shutdown/no shutdown** on the bundle.
- LFI is not supported
- Multiclass MLP is not supported
- The Cisco ASR 903 Router supports MLPPP statistics with the following limitations:

  - Packet counters on the bundle display the number of fragments rather than packets.
  - Control packets are accounted on the bundle.
- If you increase the maximum transmission unit (MTU) size on an MLPPP interface to a value higher than the maximum received reconstructed unit (MRRU) value on the peer interface, this can bring the MLPPP tunnel down. To restore the tunnel, perform a shutdown/no shutdown on the interface.

MPLS VPN Limitation

- MPLS VPN (L3VPN) Fragmentation does not function properly if an access interface has a higher MTU value than a core interface. To ensure that fragmentation functions correctly, configure the core interface MTU with a value that exceeds the access interface MTU and relevant headers.

OC-3 IM Limitations

- SDH framing mode is supported; SONET is not supported.
- Channelization is not supported.
- The optical interface module is designed for OC-3 and OC-12 traffic, but OC-12 functionality is not currently supported.

Pseudowire/AToM Limitation

- The Cisco ASR 903 Router supports ATM over MPLS N-to-one cell mode for a single ATM Virtual Channel Connections (VCCs) or Permanent Virtual Circuits (PVCs) to a pseudowire, but does not support mapping to multiple VCCs or PVCs.
- The Cisco ASR 903 Router does not support ATM over MPLS one-to-one cell mode.
- The Cisco ASR 903 Router supports pseudowire ping using the CW method; pseudowire ping using the TTL method is not supported.
- The Cisco ASR 903 Router supports a maximum of 2000 pseudowires in any combination.

QoS Limitations

For a description of QoS features and limitations on the Cisco ASR 903 Router in release 3.6S, see http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html.

Software Upgrade Limitation

- We recommend you set the **interface-module-delay** value to 150 or greater in order to ensure sufficient time for IM software upgrades.

Subinterfaces Limitation

- The Cisco ASR 903 router does not support subinterface configurations except on ATM interfaces.

Note You can configure similar functionality using multiple Ethernet Virtual Connections on an interface. For more information, see Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.

T1/E1 IM Limitations

- Inverting data on the T1/E1 interface is not supported—Inverting the data stream using the invert data interface command is not supported.

- Bit error rate test (BERT) patterns have limited support—Currently, only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported for BERT.

Limitations and Restrictions in Cisco IOS XE Release 3.6S

The following limitations apply to the Cisco ASR 903 Router in IOS XE Release 3.6S:

Note For a summary of limitations in Release 3.5S, see the IOS XE 3.5 Release Notes.

TDM Limitation

- The **configure replace** command is not supported for TDM interfaces.

EFP Limitation

- QinQ is not supported on trunk EFP interfaces.

QoS Limitations

For a description of QoS features and limitations on the Cisco ASR 903 Router in release 3.6S, see http://www.cisco.com/en/US/docs/wireless/asr_900/software/guide/chassis/Release3.6.0S/ASR903-Chassis-SW-36.html.

MLPPP Limitations

The following limitations apply when using MLPPP in IOS XE Release 3.6 on the Cisco ASR 903 Router:

- All links in an MLPPP bundle must be on the same interface module.
- All links in an MLPPP bundle must be of the same bandwidth.
- The Cisco ASR 903 Router supports a maximum of 8 links per bundle
- To change the MLPPP bundle fragmentation mode between enabled and disabled, perform a **shutdown/no shutdown** on the bundle.
- LFI is not supported
- Multiclass MLP is not supported
- The Cisco ASR 903 Router supports MLPPP statistics with the following limitations:
  - Packet counters on the bundle display the number of fragments rather than packets.
  - Control packets are accounted on the bundle.
- If you increase the maximum transmission unit (MTU) size on an MLPPP interface to a value higher than the maximum received reconstructed unit (MRRU) value on the peer interface, this can bring the MLPPP tunnel down. To restore the tunnel, perform a shutdown/no shutdown on the interface.

ATM IMA Limitation

- You can create a maximum of 16 IMA groups on each T1/E1 interface module.

Clocking and Timing Limitation

- Only a single clocking input source can be configured within each group of eight ports (0-7 and 8-15) on the T1/E1 interface module using the network-clock input-source command.

Ethernet IM Restrictions

- The Cisco ASR 903 Router does not support the Facilities Data Link (FDL) on Ethernet interfaces.
- The Cisco ASR 903 Router does not support the mac-address command on Gigabit Ethernet interface modules.
- On the Cisco ASR 903 Router, 10 Gigabit Ethernet interface modules are not supported in slots 4 and 5.
- When you install a Gigabit Ethernet IM in the topmost interface module slot (slot 5), the last interface (interface GigabitEthernet0/5/0) is not operational; the port is reserved for internal communication.

OC-3 IM Restrictions

- The **configure replace** command is not supported on the OC-3 IMs.
- SDH framing mode is supported; SONET is not supported.
- HDLC encapsulation is supported; other encapsulation types are not supported.
- Channelization is not supported.
- The optical interface module is designed for OC-3 and OC-12 traffic, but OC-12 functionality is not currently supported.

Pseudowire/AToM Limitation

- The Cisco ASR 903 Router supports ATM over MPLS N-to-one cell mode for a single ATM Virtual Channel Connections (VCCs) or Permanent Virtual Circuits (PVCs) to a pseudowire, but does not support mapping to multiple VCCs or PVCs.
- The Cisco ASR 903 Router does not support ATM over MPLS one-to-one cell mode.
- The Cisco ASR 903 Router supports pseudowire ping using the CW method; pseudowire ping using the TTL method is not supported.
- The Cisco ASR 903 Router supports a maximum of 2000 pseudowires in any combination.

Subinterfaces Limitation

- The Cisco ASR 903 router does not support subinterface configurations except on ATM interfaces.

Note You can configure similar functionality using multiple Ethernet Virtual Connections on an interface. For more information, see Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.

T1/E1 IM Limitations

- IP addresses are not supported—The current software release does not support specifying an IP address on a T1/E1 interface. You can specify an address on the interface by configuring it as a part of a CEM group using the **cem-group** command or as a part of an ATM IMA ima-group command. For more details, see the Cisco ASR 903 Series Aggregation Services Router Chassis Software Configuration Guide.
- Inverting data on the T1/E1 interface is not supported—Inverting the data stream using the invert data interface command is not supported.
- Bit error rate test (BERT) patterns have limited support—Currently, only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported for BERT.

Caveats in Cisco IOS XE 3.6S Releases

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in this chapter.

This section describes caveats in Cisco IOS XE 3.6S releases. The following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

The following sections describe the open and resolved caveats in 3.6S Releases:

Open Caveats—Cisco IOS XE Release 3.6(2)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.6(2)S.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

  Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCtw72855

  Symptoms: The router does not pass traffic towards the access side on virtual circuits (VCs) configured with QoS shaping output policy.

Conditions: Occurs when shaping is configured on class-default

Workaround: Configure shaping on user defined class

- CSCtw76473

  Symptoms: The router displays packet drops on some VPLS pseudowire virtual circuits (VCs) on the disposition side.

  Conditions: Occurs under the following conditions: -The core network is running MPLS-TP tunnels -There is an SSO switchover on the remote end or an LDP neighbor reset on the peer end.

  Workaround: There is no workaround.

- CSCty45463

  Symptoms: The router stops passing VPLS unicast traffic.

  Conditions: Occurs after you reload the router while it is passing VPLS unicast traffic.

  Workaround: Perform one of the following actions:

  – Clear the mac-address table on the affected virtual circuit (VC)

  – Stop VPLS traffic until the MAC address table is cleared, then resume VPLS traffic.

- CSCty51990

  Symptoms: The router may crash or restart; the console displays a SW_WDOG: expired message.

  Conditions: Occurs under the following conditions:

  – The router is configured with 63 or more instances of a unique EVC configured with a unique bridge domain interface (BDI).

  – The router is sending IGMP joins to one multicast group.

  – You perform a shutdown/no shutdown on the interface sending IGMP join messages.

  – You perform an OIR on the router.

  Workaround: There is no workaround.

- CSCty70119

  Symptoms: Port shaper rate changes do not take effect.

  Conditions: Occurs when QoS policies attached to EVCs on an interface do not include a shaper configuration; the issue does not occur on EFP policies that include a shaper in a class.

  Workaround: Include a shaper in one class of the EFP policy.

- CSCtz20087

  Symptoms: The router applies the class-default QoS policy to all outgoing traffic.

  Conditions: Occurs under the following conditions: -You configure multiple egress QoS policies on a Gigabit Ethernet interface. -You configure a multilink interface with no ingress QoS policy

  Workaround: There is no workaround.

- CSCua10683

  Symptoms: The router performs an RSP switchover instead of a thermal shutdown.

  Conditions: Occurs when the **facility-alarm critical exceed-action shutdown** command is in the running configuration and some sensors go into a critical condition as indicated by the **show environment all** or **show facility-alarm status** commands.

  Workaround: There is no workaround.

- CSCua13924

  Symptoms: The convergence time for IS-IS IPv4 Loop Free Alternate Fast Reroute (LFA FRR) is greater than 50 milliseconds.

  Conditions: Occurs when IS-IS LFA FRR reconverges following an interface shutdown while maintaining a large number of routes.

  Workaround: There is no workaround.

- CSCua14704

  Symptoms: The router stops passing traffic on a bridge-domain interface (BDI).

  Conditions: Occurs when you apply the **ip mtu** command to a BDI interface for the first time.

  Workaround: Remove and re-apply the **ip mtu** command.

- CSCua73104

  Symptoms: The router does not increment QoS port shaper policy counters displayed by the show policy interface command.

  Conditions: Occurs when you configure

  – A class-default policy on a physical interface

  – A class-based policy on an EVC interface

  Workaround: There is no workaround; however, the router applies the QoS policy normally.

- CSCua95777

  Symptoms: The router drops SAToP pseudowire traffic for 10 seconds following a core link failure.

  Conditions: Occurs when the TDM controller generates an AIS and LOF alarm following a core link failure; the router drops traffic for 10 seconds after generating the alarm.

  Workaround: There is no workaround.

- CSCua97383

  Symptoms: A virtual circuit (VC) with an xconnect configuration stops forwarding traffic.

  Conditions: Occurs with the 3.6(1) software under the following conditions:

  – You add and remove EFPs on an interface.

  – You remove and restore an interface configuration.

  – You are using multiple VTY sessions simultaneously to configure the router.

  Workaround: Reload the router; you can use either of the following methods to avoid this issue:

  – Use a single VTY session for configuration.

  – Apply the **configuration mode exclusive** command to prevent multiple VTYs from entering configuration mode at once.

- CSCub10414

  Symptoms: The router displays interface module (IM) traceback errors.

  Conditions: Occurs with the GLC-SX-MMD or GLC-LH-SMD (Catskills) SFPs under the following scenarios:

  – IM reload

  – SSO

  – Router reload

– SFP insertion

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.6(2)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.6(2)S.

- CSCtx00558

  Symptoms: The standby RSP crashes during bootup.

  Conditions: The issue can occur during bootup of a dual RSP system.

  Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCty22165

  Symptoms: The router displays the following console message: Transceiver initialization failed: Unable to display idprom.

  Conditions: The issue can occur when you perform an online insertion and removal (OIR) of an OC-3 interface module.

  Workaround: Perform a hard OIR (IM replacement) followed by a soft OIR (RSP switchover) on the router.

- CSCty42336

  Symptoms: BFD sessions flap on the router.

  Conditions: Occurs when the router is running IP BFD sessions in echo mode with 64 200ms X3 timers.

  Workaround: There is no workaround.

- CSCty57617

  Symptoms: The router does not update IMA interface counters.

  Conditions: Occurs after you perform an SSO on the router.

  Workaround: There is no workaround.

- CSCty74129

  Symptoms: A REP topology may reconverge during an RSP switchover. The consoles displays REP no-neighbor messages.

  Conditions: Occurs when you configure REP between two Cisco ASR 903 Routers and you perform an RSP switchover.

  Workaround: There is no workaround.

- CSCty77466

  Symptoms: The port shaper rate changes on RSP switchover.

  Conditions: Occurs under the following conditions: -You attach a shaper policy to an interface -The interface is configured with multiple EVCs -The EVC has a QoS policy attached.

Workaround: Remove and re-attach the policy on the interface.

- CSCty77704

  Symptoms: CFM traceroute fails between two CE devices.

  Conditions: Occurs under the following conditions:

  - There is a CFM xconnect between higher-level MEPs
  - The MEPs are between CE devices
  - The CE devices are in a different domain.

  Workaround: Disable CFM on the Cisco ASR 903 Router acting as a PE device.

- CSCtz03779

  Symptoms: The standby RSP crashes during ISSU.

  Conditions: Occurs when you perform an ISSU downgrade from Release 3.6 to 3.5.

  Workaround: There is no workaround.

- CSCtz54650

  Symptoms: REP flaps intermittently.

  Conditions: Occurs with a hybrid REP configuration containing ports with and without Fast LSL enabled.

  Workaround: Configure all interfaces with Fast LSL.

- CSCtz56517

  Symptoms: The router drops MPLS packets with a checksum of 0xFFFF.

  Conditions: Occurs when the ASR 903 is acting as a label disposition edge label switch router (LSR).

  Workaround: There is no workaround.

- CSCtz61153

  Symptoms: The ASR 903 does not establish BFD neighbors over port-channel 16.

  Conditions: Occurs when you configure BFD on port-channel 16 between two ASR 903 routers.

  Workaround: Configure BFD on port-channels 1 - 15.

- CSCtz75641

  Symptoms: The router drops traffic over a port-channel.

  Conditions: Occurs when you perform the following sequence of events:

  - Configure and bundle a Gigabit Ethernet interface into a port-channel
  - Remove the interface from the port-channel
  - Bundle another interface into the port-channel

  Workaround: Reload the router.

Open Caveats—Cisco IOS XE Release 3.6(1)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.6(1)S.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

  Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCtx00558

  Symptoms: The standby RSP crashes during bootup.

  Conditions: The issue can occur during bootup of a dual RSP system.

  Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCty42336

  Symptoms: BFD sessions flap on the router.

  Conditions: Occurs when the router is running IP BFD sessions in echo mode with 64 200ms X3 timers.

  Workaround: There is no workaround.

- CSCty70119

  Symptoms: Port shaper rate changes do not take effect.

  Conditions: Occurs when QoS policies attached to EVCs on an interface do not include a shaper configuration; the issue does not occur on EFP policies that include a shaper in a class.

  Workaround: Include a shaper in one class of the EFP policy.

- CSCty74129

  Symptoms: A REP topology may reconverge during an RSP switchover. The consoles displays REP no-neighbor messages.

  Conditions: Occurs when you configure REP between two Cisco ASR 903 Routers and you perform an RSP switchover.

  Workaround: There is no workaround.

- CSCty77466

  Symptoms: The port shaper rate changes on RSP switchover.

  Conditions: Occurs under the following conditions:

  – You attach a shaper policy to an interface

  – The interface is configured with multiple EVCs

  - The EVC has a QoS policy attached.

  Workaround: Remove and re-attach the policy on the interface.

- CSCtz03779

  Symptoms: The standby RSP crashes during ISSU.

  Conditions: Occurs when you perform an ISSU downgrade from Release 3.6 to 3.5.

  Workaround: There is no workaround.

- CSCtz09708

  Symptoms: The router cannot establish a PTP session when configured as a PTP slave device.

  Conditions: Occurs when the router receives PTP packets containing a VPN or VRF label.

  Workaround: There is no workaround.

- CSCtz20087

  Symptoms: The router applies the class-default QoS policy to all outgoing traffic.

  Conditions: Occurs under the following conditions: -You configure multiple egress QoS policies on a Gigabit Ethernet interface. -You configure a multilink interface with no ingress QoS policy

  Workaround: There is no workaround.

- CSCtz54650

  Symptoms: REP flaps intermittently.

  Conditions: Occurs with a hybrid REP configuration containing ports with and without Fast LSL enabled.

  Workaround: Configure all interfaces with Fast LSL.

- CSCtz56517

  Symptoms: The router drops MPLS packets with a checksum of 0xFFFF.

  Conditions: Occurs when the ASR 903 is acting as a label disposition edge label switch router (LSR).

  Workaround: There is no workaround.

- CSCtz61153

  Symptoms: The ASR 903 does not establish BFD neighbors over port-channel 16.

  Conditions: Occurs when you configure BFD on port-channel 16 between two ASR 903 routers.

  Workaround: Configure BFD on port-channels 1 - 15.

- CSCtz75641

  Symptoms: The router does not pass traffic over an EVC PC port-channel.

  Conditions: Occurs when you perform the following sequence of actions: -Remove an EVC member link from a port-channel interface -Configure a trunk EFP -Set the interface to default -Add the EVC member link back into the port-channel interface

  Workaround: Reload the router.

- CSCua03439

  Symptoms: The router displays error messages similar to the following: %EVENTLIB-3-CPUHOG: SIP0: nile_mgr:

  Conditions: Occurs when you boot the router running QoS configurations at a high scale, particularly queues.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.6(1)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.6S(1).

- CSCtu35052

  Symptoms: Sweep ping fails when an ATM interface is configured with AAL5 encapsulation.

  Conditions: Occurs when the ATM packet size is greater than 1484 bytes.

  Workaround: There is no workaround.

- CSCtw94068

  Symptoms: The router displays traceback messages, after which interfaces stop passing traffic.

  Conditions: The issue can occur when you reload the router

  Workaround: There is no workaround.

- CSCtx37768

  Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.

  Conditions: This symptom is observed when a QoS policy is applied on an EVC bridge domain interface.

  Workaround: Use one of the following workarounds:

  - Reload the router.
  - Remove and re-apply an encapsulation configuration such a VLAN.
  - Remove and re-attach the bridge domain under the EVC.
  - Perform a shutdown/no shutdown on the BDI interface.

- CSCtx73691

  Symptoms: The ASR 903 router forwards packets while in HSRP standby mode.

  Conditions: Occurs when the ASR 903 is running HSRP and the HSRP session flaps.

  Workaround: There is no workaround.

- CSCtx87145

  Symptoms: The ASR 903 router does not support LDP label packets when transmitted in PTP delay-request messages.

  Conditions: Occurs when you configure the ASR 903 router as a PTP (1588 version) boundary clock and the router sends an MPLS label packet within delay-request traffic.

  Workaround: Align the grandmaster clock source to the same IGP domain and use a prefix-list for local label filtering.

- CSCty03480

  Symptoms: The interface manager crashes when you remove a BFD template.

  Conditions: Occurs when you remove a BFD template or modify an MPLS-TP label.

  Workaround: There is no workaround.

- CSCty03617

Symptoms: The router displays the following message when executing a Stateful Switchover (SSO): %TRANSCEIVER-3-CHECKSUM_ERROR

Conditions: Occurs intermittently when the router is in SSO mode and performing a switchover between RSPs. The console displays this message repeatedly on the new active RSP.

Workaround: There is no workaround.

- CSCty26726

  Symptoms: The IOS kernel crashes.

  Conditions: Occurs following a reload on a dual RSP system.

  Workaround: Power cycle the router.

- CSCty29449

  Symptoms: The router crashes.

  Conditions: The issue can occur when you shut down and reenable an interface module.

  Workaround: There is no workaround.

- CSCty35365

  Symptoms: The router drops traffic passing across ATM MPLS layer 2 virtual circuits (VCs).

  Conditions: Occurs when you increase the scale above 100 VCs.

  Workaround: There is no workaround.

- CSCty37479

  Symptoms: The router experiences line protocol flapping on serial interfaces.

  Conditions: Occurs with the A900-IMA4OS and A900-IMA16D interface modules when the router is passing high volumes of HDLC or PPP traffic.

  Workaround: Configure the no keepalive command on serial interfaces.

- CSCty47288

  Symptoms: The router does not use a standby BITS clock source even when show commands indicate that the router has selected this clock source.

  Conditions: Occurs when you configure a standby BITS clock source as an input clock source.

  Workaround: There is no workaround.

- CSCty48493

  Symptoms: The ASR 903 may reload with when acting as a hybrid clock.

  Conditions: Occurs under the following conditions:

  - The PLL mode is TOP CLIENT
  - The session is in ACQUIRING state
  - You issue the **no ptp clock or domain 0 hybrid** command.

  Workaround: There is no workaround; however the issue occurs rarely.

- CSCty49157

  Symptoms: Some members in an IMA group do not become active even though the interface controllers are up.

  Conditions: Occurs when you perform an OIR on a remote line card or when the standby RSP becomes the active RSP.

Workaround: There is no workaround.

- CSCty51257

  Symptoms: The T1/E1 interface module changes to inserted state during an in-service software upgrade (ISSU), causing the interface to fail and the router to generate a core file.

  Conditions: Occurs when you perform an in-service software upgrade (ISSU) on a router with a T1/E1 interface module.

  Workaround: Issue the shutdown command on the interface module before beginning ISSU; after ISSU is complete, issue the no shutdown command on the interface module.

- CSCty57746

  Symptoms: On the Cisco ASR 903 router, the **show environment** command displays incorrect values, including P0 and P1 voltages and Amps values.

  Conditions: This symptom is observed with the Cisco ASR 903 router when you apply the **show environment** command.

  Workaround: There is no workaround.

- CSCty60908

  Symptoms: The ASR 903 crashes and creates a core file.

  Conditions: Occurs when the remote PE device is reloaded and an application such as VPLS or EoMPLS is running over MPLS TE FRR.

  Workaround: There is no workaround.

- CSCty61660

  Symptoms: The Cisco ASR 903 Router displays a core dump file.

  Conditions: Occurs when the remote PE device is reloaded while running VPLS-TP.

  Workaround: There is no workaround.

- CSCty71837

  Symptoms: Ping does not work properly when traversing a BDI interface.

  Conditions: Occurs when you configure MPLS on a BDI interface and ping packets are encapsulated in an MPLS header.

  Workaround: There is no workaround.

- CSCty72251

  Symptoms: The router drops traffic following a reload.

  Conditions: Occurs when you reload the router while running a VRF configuration.

  Workaround: Remove the configuration, reload the router, and re-apply the configuration.

- CSCty72901

  Symptoms: Some CEM groups do not function correctly.

  Conditions: Occurs when you configure more than 336 CEM groups on the T1/E1 or OC-3 interface module.

  Workaround: There is no workaround; avoid configuring more than 336 CEM groups.

- CSCty92979

  Symptoms: The router loses ARP table entries after a network link flaps.

Conditions: Occurs following a network link flap when the routers ARP table contains entries for next-hop neighbors connected over a router bridge domain interface.

Workaround: There is no workaround.

- CSCty93985

  Symptoms: Egress QoS policies do not take effect on an EFP interface.

  Conditions: Occurs when you apply an egress QoS policy to an interface configured with more than 37 EFPs.

  Workaround: There is no workaround.

- CSCty97391

  Symptoms: The router drops traffic for approximately 9 milliseconds.

  Conditions: Occurs on the active RSP following an HA switchover.

  Workaround: There is no workaround.

- CSCtz07388

  Symptoms: The router does not permit you to add an EFP interface to a split horizon group.

  Conditions: Occurs after you make the following configuration changes:

  - Configure 32 EFPs without a split horizon option to a bridge-domain interface.
  - Configure 2 VPLS pseudowires.

  Workaround: Configure 30 EFPs without a split horizon option, then apply the VPLS pseudowire configuration. After applying the VPLS pseudowire configuration, you can add 32 EFPs to the split horizon group.

- CSCtz17176

  Symptoms: Layer 4 port range security ACLs do not function properly.

  Conditions: Occurs when you apply port range security ACLs to an EVC interface.

  Workaround: There is no workaround.

- CSCtz38119

  Symptoms: The router does not complete a MAC address flush on the receiving side of a VPLS pseudowire.

  Conditions: Occurs when the router receives a layer 2 MAC withdrawal over a VPLS pseudowire.

  Workaround: There is no workaround.

- CSCtz40131

  Symptoms: The router does not classify traffic when using QoS ACLs.

  Conditions: Occurs when you apply a QoS ACL using the **range**, **lt**, and **gt** operators.

  Workaround: There is no workaround.

- CSCtz45069

  Symptoms: The router displays CPU hog messages or crashes.

  Conditions: Occurs under conditions in which the router or an interface module is not responding and the interface module is in an improper state.

  Workaround: There is no workaround; however the issue occurs very rarely.

- CSCtz45898

Symptoms: The router drops PTP packets.

Conditions: Occurs when PTP packets traverse a BDI with encapsulation configured.

Workaround: There is no workaround.

- CSCtz55566

  Symptoms: The router displays I2C error messages intermittently.

  Conditions: Occurs when you insert a copper SFP in the SFP interface module.

  Workaround: There is no workaround.

- CSCtz83050

  Symptoms: An interface module goes into Inserted state during ISSU.

  Conditions: Occurs when you perform an ISSU upgrade or downgrade.

  Workaround: There is no workaround.

- CSCtz96120

  Symptoms: The router does not recognize interface modules after they are reset during a software upgrade.

  Conditions: Occurs during ISSU upgrade or downgrade.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.6(0)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.6(0)S.

- CSCtr40582

  Symptoms: Ping fails.

  Conditions: Occurs when you configure AMI line code on a T1 controller.

  Workaround: There is no workaround.

- CSCts75456

  Symptoms: Multicast (S,G) entry not established.

  Conditions: Occurs when you configure OIF and IIF within BDI that are part of a trunk EFP.

  Workaround: Configure normal EVCs instead of trunk EVCs.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

  Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCtv15403

  Symptoms: 64 byte Line rate traffic not achieved.

  Conditions: Occurs with more than 11 links in a MLP bundle with A900-IMA16D interface module and packet size 64 bytes.

Workaround: There is no workaround.

- CSCtw59780

  Symptoms: BGP dynamic neighbor structures at the hub are not cleaned up after the spokes go down. The output of the **show ip bgp all sum** command continues to display dynamic neighbors.

  Conditions: This issue is observed when all the following conditions are met:

  – The scale environment for dynamic neighbors contains several thousand peers.

  – The peers are brought up and then removed before they can transition into the Established state.

  Workaround: There is no workaround.

- CSCtw94068

  Symptoms: The router displays traceback messages, after which interfaces stop passing traffic.

  Conditions: The issue can occur when you reload the router

  Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCtx37768

  Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.

  Conditions: Occurs when you apply a QoS policy on an EVC bridge domain interface.

  Workaround: Use one of the following workarounds:

  – Reload the router.

  – Remove and re-apply an encapsulation configuration such a VLAN.

  – Remove and re-attach the bridge domain under the EVC.

  – Perform a **shutdown/no shutdown** on the BDI interface.

- CSCtx38156

  Symptoms: The router crashes.

  Conditions: Occurs when you remove the **fast-reroute remote-lfa level-2 mpls-ldp** command from a configuration.

  Workaround: This command is not currently supported; avoid including it in a configuration.

- CSCtx44508

  Symptoms: There is a delay in route processor synchronization after an SSO.

  Conditions: This issue is observed when iBGP NSR is enabled and under scale conditions.

  Workaround: There is no workaround.

- CSCtx44688

  Symptoms: Cannot configure policing and marking together in the same class of the egress policy-map.

  Conditions: Set and police statements together in the same class of a policy is rejected at the CLI.

Workaround: In order to achieve marking and policing at the ingress we can use a conditional policer but this is not supported at the egress.

- CSCtx60094

  Symptoms: Type 1 MVPN routes are not created.

  Conditions: This issue is observed when the IP address of a loopback interface is changed.

  Workaround: Create a dummy neighbor under the **address-family ipv4 mvpn** configuration or the **address-family ipv6 mvpn** configuration. Alternatively, unconfigure and reconfigure the MDT group under the VRF configuration.

- CSCtx73691

  Symptoms: Standby gateway starts forwarding packet for some of the HSRP sessions.

  Conditions: This is seen on flapping the HSRP session.

  Workaround: There is no workaround.

- CSCtx75877

  Symptoms: ICMP unreachable messages are sent even though route for destination ip is present in routing table. There is no ACL applied on any of the interface.

  Conditions: This is seen on reload with VRRP configuration present on incoming interfaces.

  Workaround: There is no workaround.

- CSCtx77233

  Symptoms: The router displays an error message similar to the following:

  ```
  FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: SIP0: fman_fp_image:  frr 0x1029 download to CPP
  failed
  ```

  Conditions: Occurs when you shut down a backup tunnel and shut down an FRR-protected interface, disabling TE tunnels.

  Workaround: None; the error does not impact traffic forwarding.

- CSCtx75877

  Symptoms: ICMP unreachable messages are sent when a route for the destination ip address exists in the routing table. There is no ACL applied on any of the interface.

  Conditions: Occurs under the following conditions:

  - There is a VRRP configuration applied to incoming interfaces.
  - There are not ACLs applied on any interface.
  - Your reload the router.

  Workaround: There is no workaround.

- CSCtx77233

  Symptoms: The router displays an error message similar to the following:

  ```
  FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: SIP0: fman_fp_image:  frr 0x1029 download to CPP
  failed
  ```

  Conditions: Occurs when you shut down a backup tunnel interface and a FRR-protected interface, bringing down MPLS TE tunnels.

  Workaround: There is no workaround; the error does not appear to impact traffic forwarding.

- CSCtx80446

  Symptoms: When the **no authentication** command is run on one BFD template, other MHOP BFD sessions on which authentication has been configured may change to the Down state.

  Conditions: This issue is observed when there are multiple sessions that use different maps and templates.

  Workaround: There is no workaround.

- CSCtx81871

  Symptoms: MPLS convergence time is higher than normal.

  Conditions: Occurs when the router is processing more than 3107 iBGP and label prefixes.

  Workaround: There is no workaround.

- CSCty03480

  Symptoms: The interface manager crashes when you remove a BFD template.

  Conditions: Occurs when you remove a BFD template or modify an MPLS-TP label.

  Workaround: There is no workaround.

- CSCty03617

  Symptoms: The router displays the following message when executing a Stateful Switchover (SSO): `%TRANSCEIVER-3-CHECKSUM_ERROR`

  Conditions: Occurs intermittently when the router is in SSO mode and performing a switchover between RSPs. The console displays this message repeatedly on the new active RSP.

  Workaround: There is no workaround.

- CSCty13332

  Symptoms: An imposition failure occurs on VCs configured with MPLS TP LSPs.

  Conditions: Occurs under the following conditions:

  - There are input and output QoS policy-maps configured on service instance interfaces.
  - The router is configured with 255 MPLS TP tunnels.
  - The router is configured with a high number of virtual circuits (VCs).
  - The RSP in slot 0 is acting as the active RSP.
  - An event occurs that causes the router to tear down and rebuild all MPLS TP tunnels and VCs at once.

  Workaround: Remove and reconfigure the service instance.

- CSCty13699

  Symptoms: When L2VPN Pseudowire Stitching is configured between a static segment and a dynamic segment, both segments may move to the Down state.

  Conditions: This issue is observed when L2VPN Pseudowire Stitching is configured between a static segment and a dynamic segment.

  Workaround: There is no workaround.

- CSCty22165

  Symptoms: The router displays the following console message: `Transceiver initialization failed: Unable to display idprom`.

Conditions: The issue can occur when you perform an online insertion and removal (OIR) of an OC-3 interface module.

Workaround: Perform a hard OIR (IM replacement) followed by a soft OIR (RSP switchover) on the router.

- CSCty24143

  Symptoms: The router does not pass IPv6 OSPF traffic.

  Conditions: Occurs when the router passes traffic at the full line rate of a link.

  Workaround: Reduce the traffic rate by 10%.

- CSCty26726

  Symptoms: The IOS kernel crashes.

  Conditions: Occurs following a reload on a dual RSP system.

  Workaround: Power cycle the router.

- CSCty28986

  Symptoms: A configuration with a high number of down MEPs does not function properly.

  Conditions: Occurs when you configure 500 or more down MEPs with 500 or more xconnect configurations between service instances.

  Workaround: Configure no more than 300 CFM sessions.

- CSCty29449

  Symptoms: The router crashes.

  Conditions: The issue can occur when you shut down and reenable an interface module.

  Workaround: There is no workaround.

- CSCty34054

  Symptoms: The router displays CPU utilization traceback messages and drops all multicast traffic for 20–50 seconds.

  Conditions: Occurs under the following conditions:

  - Multicast is enabled with more than 500 multicast groups
  - The router is using RSP1B in SSM mode
  - BDI is configured on the access side of the router
  - There are 24 EFPs on each bridge domain
  - You enter a **shutdown** command on the access interface.

  Workaround: There is no workaround.

- CSCty34521

  Symptoms: The router does not pass CFM traffic over an Ethernet CFM cross-connect.

  Conditions: Occurs under the following conditions:

  - There is a CFM xconnect between two Cisco ASR 903 Router devices
  - You perform an OIR and set a default interface.

  Workaround: Do not continuously perform an OIR and set a default interface.

- CSCty34812

  Symptoms: The router experiences traffic loss for between 10 and 50 seconds during RSP switchover.

  Conditions: Occurs when you perform an RSP switchover on a router with a ten gigabit Ethernet interface module.

  Workaround: There is no workaround.

- CSCty35365

  Symptoms: The router drops traffic passing across ATM MPLS layer 2 virtual circuits (VCs).

  Conditions: Occurs when you increase the scale above 100 VCs.

  Workaround: There is no workaround.

- CSCty37479

  Symptoms: The line protocol repeatedly drops (flaps) on serial interfaces.

  Conditions: Occurs when you configure HDLC or PPP on serial interfaces on the A900-IMA4OS or A900-IMA16D interface modules when the router is passing high traffic volumes.

  Workaround: Configure the **no keepalive** command on serial interfaces.

- CSCty38638

  Symptoms: The router cannot download the ACL database.

  Conditions: Occurs when the router is configured with an ACL containing more than 400 access control entries (ACEs).

  Workaround: There is no workaround.

- CSCty39033

  Symptoms: Interface modules stop passing traffic during an RSP switchover.

  Conditions: Occurs when the router switches over to the standby RSP while traffic is passing on interface modules.

  Workaround: There is no workaround.

- CSCty41536

  Symptoms: The router crashes during when SNMP uses a high percentage of CPU for an extended period.

  Conditions: Occurs when SNMP is running the background with an average of 50% CPU utilization for more than 8 hours.

  Workaround: Reduce the load on the CPU using SNMP poll and SNMP walk.

- CSCty42336

  Symptoms: BFD sessions flap on the router.

  Conditions: Occurs when the router is running IP BFD sessions in echo mode with 64 200ms X3 timers.

  Workaround: There is no workaround.

- CSCty42867

  Symptoms: The router crashes.

  Conditions: Occurs when you apply traffic soaking to the router with L2VPN services configured.

  Workaround: There is no workaround.

- CSCty44345

  Symptoms: The router experiences packet drops when passing 64 byte packets.

  Conditions: Occurs when the router is passing 64 byte packets at the line rate on the OC-3 interface module.

  Workaround: Configure a larger packet size on the interface.

- CSCty45058

  Symptoms: Some CEM groups do not function correctly.

  Conditions: Occurs when you configure more than 196 CEM groups on the T1/E1 or OC-3 interface module.

  Workaround: There is no workaround; avoid configuring more than 196 CEM groups.

- CSCty45463

  Symptoms: The router stops passing VPLS unicast traffic.

  Conditions: Occurs after you reload the router while it is passing VPLS unicast traffic.

  Workaround: Perform one of the following actions:

  – Clear the mac-address table on the affected virtual circuit (VC)

  – Stop VPLS traffic until the MAC address table is cleared, then resume VPLS traffic.

- CSCty46058

  Symptoms: Shutting down a static multisegment VFI causes traffic to flow in one direction.

  Conditions: This issue is observed when you configure a point-to-point VFI with two static neighbors and then shut down the VFI by using the **shutdown** command.

  Workaround: There is no workaround.

- CSCty48710

  Symptoms: The router drops multicast packets on layer 3 interfaces.

  Conditions: Occurs when you configure 63 bridge domains per port and the router sends IGMP joins from all of the bridge domains to the same IGMP group.

  Workaround: You can apply the following workarounds:

  – Applying a policy-map on each EVC can reduce the packet drops to some extent.

  – Increase the default port queue size.

- CSCty49041

  Symptoms: The router drops VPLS traffic on one or more virtual circuits (VCs).

  Conditions: Occurs when you reload a CPE or UPE device when there approximately 100 VCs configured between the UPE and NPE devices.

  Workaround: Issue the **clear xconnect** command on the affected VC.

- CSCty49157

  Symptoms: Some members in an IMA group do not become active even though the interface controllers are up.

  Conditions: Occurs when you perform an OIR on a remote line card or when the standby RSP becomes the active RSP.

  Workaround: There is no workaround.

- CSCty50377

Symptoms: The OC-3 interface module crashes when you perform multiple RSP switchovers.

Conditions: Occurs when the router is running a CEM configuration configured at full scale on all ports and passing traffic.

Workaround: There is no workaround.

- CSCty51175

  Symptoms: Serial interfaces configured with HDLC display false LOF or AIS alarms.

  Conditions: Occurs when you configure a high volume of serial interfaces using HDLC.

  Workaround: Remove and re-apply the serial interface configuration.

- CSCty51257

  Symptoms: The T1/E1 interface module changes to inserted state during an in-service software upgrade (ISSU), causing the interface to fail and the router to generate a core file.

  Conditions: Occurs when you perform an in-service software upgrade (ISSU) on a router with a T1/E1 interface module.

  Workaround: Issue the shutdown command on the interface module before beginning ISSU; after ISSU is complete, issue the no shutdown command on the interface module.

- CSCty51984

  Symptoms: CEM circuits become inactive.

  Conditions: Occurs when you perform an OIR, reload, or when you reconfigure a CEM circuit on the router. The issue occurs more consistently when the router is running more than 300 CEM circuits.

  Workaround: Issue the **clear xconnect all** command.

- CSCty51990

  Symptoms: The router may crash or restart; the console displays a `SW_WDOG: expired` message.

  Conditions: Occurs under the following conditions:

  - The router is configured with 63 or more instances of a unique EVC configured with a unique bridge domain interface (BDI).
  - The router is sending IGMP joins to one multicast group.
  - You perform a shutdown/no shutdown on the interface sending IGMP join messages.
  - You perform an OIR on the router.

  Workaround: There is no workaround.

- CSCty57746

  Symptoms: The **show environment** command displays incorrect values, including P0 and P1 voltages, PSU status, PSU voltage, and critical alarms.

  Conditions: Occurs when you apply the **show environment** command.

  Workaround: There is no workaround.

- CSCty57751

  Symptoms: The router crashes.

  Conditions: Occurs under any of the following conditions:

  - You perform an OIR on an interface module.
  - You issue the no ppp multilink command on all MLP member links.

  - You set the MTU to a higher value on an MLP bundle.

  Workaround: There is no workaround.

- CSCty61660

  Symptoms: The Cisco ASR 903 Router displays a core dump file.

  Conditions: Occurs when the remote PE device is reloaded while running VPLS-TP.

  Workaround: There is no workaround.

- CSCty66871

  Symptoms: The router stops forwarding traffic across one or more EoMPLS virtual circuits (VC)s**.**

  Conditions: Occurs when you perform a shut/no shutdown on the MPLS TE tunnel carrying the VC.

  Workaround: Issue the clear xconnect command on the VC.

- CSCty70034

  Symptoms: The router floods all EFPs in the sam e split horizon group with IGMP join messages.

  Conditions: Occurs when the router is sending an IGMP join containing a dot1q tag for one EVC.

  Workaround: None.

- CSCty72251

  Symptoms: The router drops traffic following a reload.

  Conditions: Occurs when you reload the router while running a VRF configuration.

  Workaround: Remove the configuration, reload the router, and re-apply the configuration.

- CSCty72901

  Symptoms: Some CEM groups do not function correctly.

  Conditions: Occurs when you configure more than 196 CEM groups on the T1/E1 or OC-3 interface module.

  Workaround: There is no workaround; avoid configuring more than 196 CEM groups.

- CSCty73142

  Symptoms: An IPC Init failure occurs during downgrade, which makes the standby reload continuously.

  Conditions: Occurs when you perform an ISSU downgrade from IOS XE 3.6 to IOS XE 3.5.1 or 3.5.

  Workaround: There is no workaround.

- CSCty73362

  Symptoms: The router experiences CPP download failures when sending IGMP join messages.

  Conditions: Occurs when the router is configured with a trunk EFP in SM mode on the access side and is sending IGMP join messages to more than 1970 multicast groups.

  Workaround: There is no workaround.

- CSCty73365

  Symptoms: The router drops traffic on ATM subinterfaces using layer 2 PVCs.

  Conditions: Occurs when you create 255 or more ATM PVCs.

  Workaround: There is no workaround.

- CSCty73528

  Symptoms: The router displays core dump files.

  Conditions: Occurs when you perform an RSP switchover when CEF routes are configured.

  Workaround: There is no workaround.

- CSCty74058

  Symptoms: The router sends traffic for virtual circuits (VCs) over Gigabit Ethernet interfaces instead of MPLS-TP tunnels.

  Conditions: Occurs when you perform an interface module OIR and the VCs are configured with a preferred path as the MPLS-TP tunnel.

  Workaround: There is no workaround.

- CSCty74062

  Symptoms: The router does not pass MLP traffic.

  Conditions: Occurs when you perform an RSP switchover with an existing MLP configuration.

  Workaround: There is no workaround.

- CSCty74129

  Symptoms: A REP topology may reconverge during an RSP switchover. The consoles displays REP no-neighbor messages.

  Conditions: Occurs when you configure REP between two Cisco ASR 903 Routers and you perform an RSP switchover.

  Workaround: There is no workaround.

- CSCty77704

  Symptoms: CFM traceroute fails between two CE devices.

  Conditions: Occurs under the following conditions:

  - There is a CFM xconnect between higher-level MEPs
  - The MEPs are between CE devices
  - The CE devices are in a different domain.

  Workaround: Disable CFM on the Cisco ASR 903 Router acting as a PE device.

- CSCty79273

  Symptoms: Multicast replication does not occur on all BDI interfaces on a given trunk EFP.

  Conditions: Occurs under the following conditions:

  - The router is configured with 63 or more BDIs
  - The BDIs are configured as OIFs on a trunk EFP.
  - The port on which the EFP is configured is in a multicast group.

  Workaround: There is no workaround.

- CSCty80326

  Symptoms: The router displays an Eamapper error.

  Conditions: Occurs under the following conditions:

  - The router is configured with a port channel interface with 2 member links.
  - The port channel

  - The configuration contains 48 EFPs with 24 EFPs in a given bridge domain
  - SSM is enabled on the local and a remote router
  - The router sends an IGMP join to a single multicast group.

  Workaround: There is no workaround.

- CSCty87424

  Symptoms: The router experiences a drop in forwarded packets on an MLPPP bundle.

  Conditions: Occurs when the bundle is using 64% or more of the available bandwidth and an MTU value is configured on the bundle.

  Workaround: There is no workaround.

- CSCty90425

  Symptoms: The router crashes and reboots.

  Conditions: Occurs when you perform a longevity test with traffic soaking while using Ethernet features such as EoMPLS, VPLS, CFM, or Y1731.

  Workaround: There is no workaround.

- CSCty92979

  Symptoms: The router loses ARP table entries after a network link flaps.

  Conditions: Occurs following a network link flap when the router's ARP table contains entries for next-hop neighbors connected over a router bridge domain interface.

  Workaround: There is no workaround.

- CSCty93985

  Symptoms: Egress QoS policies do not take effect on an EFP interface.

  Conditions: Occurs when you apply an egress QoS policy to an interface configured with more than 37 EFPs.

  Workaround: There is no workaround.

- CSCty94081

  Symptoms: The router displays an EgBridgeError_0 error when sending multicast traffic.

  Conditions: Occurs in the following conditions:

  - There are 40 bridge domain interfaces (BDIs) sending IGMP joins to a single multicast group.
  - There are more than 40 OIFs and 24 EVCs in each bridge domain.

  Workaround: There is no workaround.

- CSCty94437

  Symptoms: The router crashes during RSP switchover or bootup.

  Conditions: Occurs when L2VPN services are passing bidirectional traffic on the router and you perform a reload or RSP switchover.

  Workaround: There is no workaround.

- CSCty96326

  Symptoms: The router crashes.

  Conditions: Occurs during bootup when the router is running BFD and CFM sessions that are offloaded to hardware.

Workaround: There is no workaround.

- CSCty96797

  Symptoms: L2 OIF replication does not take effect when you add or delete an EVC.

  Conditions: Occurs after a bridge domain or split horizon group change.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.6(0)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.6(0)S.

- CSCtx47195

  Symptoms: BFD flaps when you perform a RSP switchover.

  Conditions: Occurs under the following conditions:

  - The router is configured as a mid-point node.
  - The router is running MPLS-TP sessions with BFD.
  - You perform a soft OIR.

  Workaround: None.

- CSCtx83922

  Symptoms: Interfaces go into a down-down state.

  Conditions: The issue can occur when you use a script to implement a full-scale configuration.

  Workaround: Perform an RSP switchover on both sides of the connection.

- CSCty04161

  Symptoms: The RSP is unable to modify the configuration file or execute show interface commands.

  Conditions: Occurs following an RSP switchover.

  Workaround: None.

- CSCty43582

  Symptoms: The router does not save the **port-channel load-balance-hash-algo** command in the running configuration.

  Conditions: Occurs when you select the **src-ip**, **dst-ip**, or **src-dst-ip** hash algorithm.

  Workaround: None.

- CSCty44236

  Symptoms: Traffic switches over the protect-lsp of a mpls-tp tunnel interface, even though corresponding working-lsp link is active.

  Conditions: Occurs when the protect-lsp bfd goes down while the protect lsp out-link interface going down.

  Workaround: None.

- CSCty58020

  Symptoms: Policy-map counters do not function properly.

  Conditions: Occurs when you configure an ACL-based class-map under a policy-map.

Workaround: None.

Restrictions and Caveats in Cisco IOS XE 3.7S Releases

This chapter provides information about restrictions and caveats in Cisco IOS XE 3.7S releases.

Note Because Cisco IOS XE 37S is based on Cisco IOS XE 3.5 inherited releases, some caveats that apply to Cisco IOS XE 3.5 releases also apply to Cisco IOS XE 37S. Release 3.5 is not described in this document; for a list of the software caveats that apply to Cisco IOS XE 3.5, see the Release Notes for Cisco IOS XE Release 3S.

Note We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

This chapter contains the following sections:

Limitations and Restrictions

The following sections describe the Cisco ASR 903 Router limitations in IO S XE 3.7 releases:

Limitations and Restrictions in Cisco IOS XE Release 3.7(4)S

There are no changes in limitations and restrictions in Cisco IOS XE Release 3.7(4)S; the restrictions from IOS XE Release 3.7(2)S still apply.

Limitations and Restrictions in Cisco IOS XE Release 3.7(3)S

There are no changes in limitations and restrictions in Cisco IOS XE Release 3.7(3)S; the restrictions from IOS XE Release 3.7(2)S still apply.

Limitations and Restrictions in Cisco IOS XE Release 3.7(2)S

The following limitations and restrictions apply to Cisco IOS XE Release 3.7(2)S for the Cisco ASR 903 Router:

- LFA FRR Limitations—Release 3.7.2 has the following limitations for Loop Free Alternate Fast-reroute (LFA FRR):
  - To enable LFA FRR, you must include the **mpls ldp explicit-null** command. The implicit-null command is not supported.
  - LFA FRR is not supported with equal cost multipath (ECMP).
  - The ASR 903 supports up to 4000 LFA FRR routes.
  - Remote LFA tunnels are not HA aware; hence they are SSO co-existent but not SSO compliant.
- The restrictions from IOS XE Release 3.7(0)S apply to Release 3.7(2). For more information, see Limitations and Restrictions in Cisco IOS XE Release 3.7(0)S, page 2.

Limitations and Restrictions in Cisco IOS XE Release 3.7(1)aS

There are no changes in limitations and restrictions in Cisco IOS XE Release 3.7(1)aS; the restrictions from IOS XE Release 3.7(0)S still apply.

Limitations and Restrictions in Cisco IOS XE Release 3.7(0)S

The following limitations apply to the Cisco ASR 903 Router in IOS XE Release 3.7(0)S:

TDM Limitation

- The **configure replace** command is not supported for TDM interfaces.

ATM IMA Limitation

- You can create a maximum of 16 IMA groups on each T1/E1 interface module.

Bridge Domain Interface Limitation

- The **mtu** command is not supported on BDI interfaces; however the **ip mtu** command is supported.

Clocking and Timing Limitation

- Only a single clocking input source can be configured within each group of eight ports (0-7 and 8-15) on the T1/E1 interface module using the network-clock input-source command.
- Synchronous Ethernet clock sources are not supported with PTP. Conversely, PTP clock sources are not supported with synchronous Ethernet. However, you can use hybrid clocking to allow the router to obtain frequency using Synchronous Ethernet and phase using PTP.

EFP Limitation

- QinQ is not supported on trunk EFP interfaces.

Equal Cost Multipath Limitation

- The ASR 903 supports a maximum of 4 Equal Cost Multipath (ECMP) links.

Ethernet IM Limitations

- The Cisco ASR 903 Router does not support the Facilities Data Link (FDL) on Ethernet interfaces.
- The Cisco ASR 903 Router does not support the **mac-address** command on Gigabit Ethernet interface modules.
- 10 Gigabit Ethernet interface modules are not supported in slots 4 and 5.
- When you install a Gigabit Ethernet IM in the topmost interface module slot (slot 5), the last interface (interface GigabitEthernet0/5/0) is not operational; the port is reserved for internal communication.
- When you configure the copper and SFP Gigabit Ethernet interface modules on a router with redundant RSPs, the **speed** and **duplex** commands are not visible in interface configuration mode until you apply a **shutdown/no shutdown** to the interface.
- LACP Fast-Switchover Limitation—Cisco IOS has a default carrier-delay value of 2 seconds. When an LACP link fails, the router does not perform a switchover until the carrier-delay timer expires. The **carrier-delay** command helps reduce this value. We recommend that you set a **carrier-delay** value of greater than 0 as this value can result in slower convergence times. We also recommend that you set an identical **carrier-delay** value on all LACP member links.

MLPPP Limitations

The following limitations apply when using MLPPP on the Cisco ASR 903 Router:

- All links in an MLPPP bundle must be on the same interface module.
- All links in an MLPPP bundle must be of the same bandwidth.
- The Cisco ASR 903 Router supports a maximum of 8 links per bundle
- To change the MLPPP bundle fragmentation mode between enabled and disabled, perform a **shutdown/no shutdown** on the bundle.
- LFI is not supported
- Multiclass MLP is not supported
- The Cisco ASR 903 Router supports MLPPP statistics with the following limitations:
  - Packet counters on the bundle display the number of fragments rather than packets.
  - Control packets are accounted on the bundle.
- If you increase the maximum transmission unit (MTU) size on an MLPPP interface to a value higher than the maximum received reconstructed unit (MRRU) value on the peer interface, this can bring the MLPPP tunnel down. To restore the tunnel, perform a shutdown/no shutdown on the interface.

MPLS VPN Limitation

- MPLS VPN (L3VPN) Fragmentation does not function properly if an access interface has a higher MTU value than a core interface. To ensure that fragmentation functions correctly, configure the core interface MTU with a value that exceeds the access interface MTU and relevant headers.

OC-3 IM Limitations

- The **configure replace** command is not supported on the OC-3 IMs.
- SDH framing mode is supported; SONET is not supported.
- The optical interface module is designed for OC-3 and OC-12 traffic, but OC-12 functionality is not currently supported.
- If you issue the **no card type** command on the controller, you must reload the router in order to configure a new **card type** value.
- We recommend that you use Release 3.7.2 or later when using the OC-3 IM with high availability (HA) features such as stateful switchover (SSO).

Pseudowire/AToM Limitation

- The Cisco ASR 903 Router supports ATM over MPLS N-to-one cell mode for a single ATM Virtual Channel Connections (VCCs) or Permanent Virtual Circuits (PVCs) to a pseudowire, but does not support mapping to multiple VCCs or PVCs.
- The Cisco ASR 903 Router does not support ATM over MPLS one-to-one cell mode.
- The Cisco ASR 903 Router supports pseudowire ping using the CW method; pseudowire ping using the TTL method is not supported.
- The Cisco ASR 903 Router supports a maximum of 2000 pseudowires in any combination.

QoS Limitations

- For a description of QoS features and limitations on the Cisco ASR 903 Router in release 3.7S, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.7.0S/ASR903-Chassis-SW-37.html.

Software Upgrade Limitation

- We recommend you set the **interface-module-delay** value to 150 or greater in order to ensure sufficient time for IM software upgrades.

Subinterfaces Limitation

- The Cisco ASR 903 router does not support subinterface configurations except on ATM interfaces.

Note You can configure similar functionality using multiple Ethernet Virtual Connections on an interface. For more information, see Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.

T1/E1 IM Limitations

- Inverting data on the T1/E1 interface is not supported—Inverting the data stream using the invert data interface command is not supported.
- Bit error rate test (BERT) patterns have limited support—Currently, only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported for BERT.

Caveats in Cisco IOS XE 3.7S Releases

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in this chapter.

This section describes caveats in Cisco IOS XE 3.7S releases.

In this section, the following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

The following sections describe the open and resolved caveats in 3.7S Releases:

Open Caveats—Cisco IOS XE Release 3.7(4)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.7(4)S.

- CSCtw92458

  Symptom: IFM CC messages are leaked to unmatched encapsulation on that bridge domain (BD).

  Conditions: This issue occurs when EVCs with different encapsulation are present on same BD.

  Workaround: There is no workaround.

- CSCty63969

  Symptom: Ping fails to remote MEP.

  Conditions: This issue occurs when CFM is configured and a ping to remote MEP with packet size greater than 1478 bytes is executed.

  Workaround: There is no workaround.

- CSCua77688

  Symptom: The router experiences remote CFM MEP flapping.

  Conditions: Occurs when the router is connected via a CFM xconnect and the link is running a high traffic rate.

  Workaround: Reduce the rate of traffic.

- CSCua99096

  Symptoms: The **show ima interface** command omits some IMA group information such as ImaGroupSymmetry.

  Conditions: This issue occurs when the **show ima interface** command.

  Workaround: There is no workaround.

- CSCub94462

  Symptom: The router displays object download error messages on the console.

  Conditions: This issue occurs under the following conditions

  - Execute the **mac address sticky** command.
  - Configure 25 incremental MAC addresses and execute the **clean mac-address-table bdomain** command
  - Remove a mac security sticky configuration from an EVC interface.

  Workaround: Avoid issuing the **clear mac-address-table** command when the **mac security sticky** command is applied.

- CSCuc08397

  Symptom: When IFM is configured on EVC BD, with encapsulation default in the core, the remote MEPS are not learnt.

  Conditions: This issue is seen when encapsulation default is configured on the core facing side.

  Workaround: There is no workaround.

- CSCud09142

  Symptom: FP active error messages are seen when the tunnel-tp interface is removed in a high-availability setup.

  Conditions: This issue is seen after removing tunnel-tp interface.

  Workaround: There is no workaround.

- CSCud34600

  Symptom: Event hog messages are received when 21k to 25k routes are advertised into MBGP and exported from one PE to another.

  Conditions: This issue occurs when the redistributing routes range from 21k to 25k routes from OSFP are moved into MBGP and are exported from one PE to another.

  Workaround: There is no workaround.

- CSCud90362

  Symptom: the SYNC packets go out quite irregularly when PTP master is configured.

  Conditions: This issue is seen when the router is configured as PTP master.

  Workaround: There is no workaround.

- CSCue24854

  Symptom: Loss of 70 msec are observed when performing an IM OIR in a remote LFA ring.

  Conditions: This issue occurs when soft OIR is performed.

  Workaround: Do a hard OIR to get less than 50 msec loss.

- CSCue73478

  Symptom: The standby RSP Sync LED become holdover after switchover.

  Conditions: This issue occurs in normal conditions,

  Workaround: There is no workaround. This issue is cosmetic.

- CSCue96886

  Symptom: Complete MAC Address space is not available on the RSP.

  Conditions: This issue occurs after removing the service instance with the MAC Addresses learnt on the BD.

  Workaround: Shutdown the service instance corresponding to bridge-domain and clear the MAC-address-table of that bridge-domain. Remove the service instance.

- CSCuf07508

  Symptom: The Gigabit Ethernet port on IMA8S may not come up after reload.

  Conditions: This issue occurs when the router is reloaded multiple times

  Workaround: Perform an IM OIR.

- CSCuf44077

  Symptom: The show interface command output displays incorrect speed values after SSO.

  Conditions: This issue occurs when 100M SFPs are used

  Workaround: Perform hardware module reset.

- CSCuf86247

  Symptom: SNMP MIB variables related to BDI counters do not function properly.

  Conditions: This issue occurs when SNMP MIB variables related to BDI interface counters are used.

  Workaround: There is no workaround.

- CSCuh46103

  Symptom: The BDI statistics not getting incremented.

  Conditions: This issue is observed when the **show interface bdi statistics** command is executed. The ingress and egress statistics displayed do not get incremented even if the traffic is going through the BDI interface.

  Workaround: Use **show platform hardware pp active interface statistics bdi** command to view the statistics.

- CSCuh65489

Symptom: The BGP session goes down when ICMP echo-request of 1500 pps is received.

Conditions: This issue occurs when the router has BGP peers and receives the ICMP-echo request. The BGP hold timer expires nd BGP peer goes down.

Workaround: There is no workaround.

- CSCuh79730

  Symptom: The transmitting frequency is incorrectly displayed in case of DWDM-XFP-C.

  Conditions: This issue occurs when **show hw-module subslot 0 transceiver idprom** command is executed.

  Workaround: There is no workaround.

- CSCui50862

  Symptom: Few CFM primary sessions stays inactive.

  Conditions: This issue occurs when CFM domain with SLA is configured.

  Workaround: There is no workaround.

- CSCui87257

  Symptom: The interface clock is not detected after a switchover

  Conditions: This issue occurs after a switvchover is performed from RSP0 to RSP1.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.7(4)S

This section documents the resolved caveats for the Cisco ASR 903 Router in Cisco IOS XE Release 3.7(4)S

- CSCtz43467

  Symptom: All commands listed under the REP configuration modes cannot be configured. This was seen while configuring REP with BDI and configuring more than one source ports in a span session.

  Conditions: This issue occurs in normal working conditions.

  Workaround: There is no workaround.

- CSCua95675

  Symptom: An Ethernet virtual circuit (EVC) interface stops forwarding traffic.

  Conditions: This issue occurs when multiple EVCs are configured on a single interface. The EVCs have the same outer tag VLAN.When one of the EVCs is removed from the configuration, the other EVCs with the same outer tag VLAN stop passing traffic.

  Workaround: Issue a **shutdown** command followed by a **no shutdown** command on the Ethernet interface.

- CSCuc60148

  Symptom: System does not shut down when the temperature sensor reaches shutdown threshold region.

  Conditions: This issue occurs when the temperature sensors reaches the shutdown threshold region.

Workaround: Configure the **facility-alarm critical exceed-action shutdown** command has to enable this system shutdown behavior.

- CSCud61551

  Symptom: Serial Number of the RSP in slot 1 is not displayed some times in the **show inventory** command output.

  Conditions: This issue occurs under normal working conditions.

  Workaround: Reload the router again.

- CSCue24621

  Symptom: When one EFP is shut, traffic get stops for other EVCs.

  Conditions: This issue occurs where there are multiple qinq EFPs with same outer vlan tag on one interface.

  Workaround: There is no workaround.

- CSCue25349

  Symptom: Tracebacks seen on the router with inject bypass set to OFF.

  Conditions: This issue occurs after shutting down the core facing interface or any OSPF enabled interface.

  Workaround: There is no workaround.These traces does not have any functional impact.

- CSCue51682

  Symptom: The REP protocol flaps, as indicated by the following error messages:

  ```
  *Feb 8 06:51:38.857: %REP-4-LINKSTATUS: GigabitEthernet0/0/1 (segment 10) is
  non-operational due to neighbor not responding *Feb 8 06:51:39.096: %REP-4-LINKSTATUS:
  GigabitEthernet0/0/1 (segment 10) is operational
  ```

  Conditions: This issue occurs under the following conditions:

  - The router is sending traffic using the incremental MAC address table Fast LSL is configured using a 200ms timer.
  - The router is configured with more than 2000 MAC addresses.

  Workaround: Remove fast LSL from the REP configuration.

- CSCue60699

  Symptom: The router auto-negotiates full duplex with 1000M half/full duplex configuration.

  Conditions: This issue occurs when the router has Copper SFP with auto-negotiate enabled. and SFP is configured with 1000M half-duplex mode.

  Workaround: There is no workaround.

- CSCue61803

  Symptom: The interface modules do not get powered off, when router is reloaded.

  Conditions: This issue is occasionally seen on reload.

  Workaround: There is no workaround.

- CSCue61850

  Symptom: Memory allocation observed fro CFM EVC BD offload cases- scale configurations

  Conditions: This issue occurs with CFM EVC BD, when 256 session of3.3ms interval and 256 SLM session are configured and a **shutdown** command followed by a **no shutdown** command is issued on the traffic sending interface.

  Workaround: Configure CFM session between 50-100.

- CSCue67835

  Symptom: OSPF flap with aggressive timers (2 sec hello interval, 6 sec dead interval).

  Conditions: This issue occurs on router Stateful switchover (SSO).

  Workaround: Use the default OSPF hello timers.

- CSCue75372

  Symptom: Time-hog traceback seen on router reload or IM reload.

  Conditions: This issue occurs on router bootup or IM bootup.

  Workaround: There is no workaround.

- CSCue77596

  Symptom: CoS value gets wrongly marked for a qinq packet.

  Conditions: This issue occurs when a service instance with dot1q encapsulation and **no rewrite** is configured on the interface; The policy map attached in the ingress has marking configured.

  Workaround: There is no workaround.

- CSCue80866

  Symptom: Label exhaustion message is seen with scale match vlan and match PHB policy; Classification fails to work.

  Conditions: This issue occurs with TEFP with range of BDs that have match VLANs of the corresponding BD and a child policy to match prec/cos.

  Workaround: There is no workaround.

- CSCue83621

  Symptom: Policy-map stops working on removing class default class dynamically.

  Conditions: This issue occurs when policy-map is attached to target and class-default of top level is deleted dynamically.

  Workaround: Detach and reattach the policy-map on target.

- CSCue91533

  Symptom: Traffic through VPLS pseudowire is flooded due to MAC aging.

  Conditions: This symptom is observed when bridge descriptor index (internal index) assigned to MAC address exceeds 20480.

  Workaround: There is no workaround.

- CSCue94811

  Symptom: Process crash on standby router would not generate a core file.

  Conditions: This issue occurs under normal conditions.

  Workaround: There is no workaround.

- CSCuf02518

  Symptom: IPv4 traffic gets affected on IPv6 ACL applied interface.

  Condition: This issue occurs when both If IPv4 and IPv6 ACLs share the same label, the IPv4 traffic on the interface on which IPv6 ACL is applied is impacted.

  Workaround: There is no workaround.

- CSCuf43992

  Symptom: The router crashed with local span configuration.

  Conditions: This issue occurs with local span configuration.

  Workaround: Configure erspan configuration with source and destination erspan sessions in the router.

- CSCuf51509

  Symptom: WRED counters for CS0 does not work in **show policy-map interface** command.

  Conditions: This issue is observed when **show policy-map interface** command is executed.

  Workaround: There is no workaround.

- CSCuf53527

  Symptom: Cos inner value gets copied into the cos value.

  Conditions: This issue occurs when QinQ without rewrite service instance is configured.

  Workaround: Apply the qos policy-map to the cos inner value.

- CSCuf56723

  Symptom: The interface LED glows green when shut.

  Conditions: This issue occurs after an SSO is performed.

  Workaround: There is no workaround.

- CSCuf65301

  Symptom: Micro flaps observed on the router.

  Conditions: This issue is seen when system is kept idle for hours.

  Workaround: There is no workaround

- CSCuf79397

  Symptom: F1 is stuck in init state after the standby RSP reloads.

  Conditions: This issue occurs on a reload or OIR of the standby RSP.

  Workaround: Reload the standby RSP again.

- CSCuf83886

  Symptom: Label exhaust message is seen even on valid case if policy is configured before xconnect is configured on scaled configuration.

  Conditions: This issue occurs when a service-policy is configured before configuring xconnect on the router that has consumed close to max labels.

  Workaround: First configure xconnect and then configure service-policy.

- CSCug05239

  Symptom: Traffic drops on the router.

  Conditions: This issue occurs when configuring multichassis Link Aggregation Control Protocol (MLACP) switchover with Ethernet over Multiprotocol Label Switching (EOMPLS).

  Workaround: Configure port channel with EOMPLS.

- CSCug05647

  Symptom: Interface counters do not get updated with IP traffic.

  Conditions: This issue occurs when pinging back to back connected interfaces; the interface counters stay at 0.

  Workaround: Reload the device

- CSCug18630

  Symptom: When you perform an OIR on the standby and active RSPs, CMAND crashes.

  Conditions: This issue is observed after performing multiple standby OIRs and bringing the standby machine up.

  Workaround: There is no workaround.

- CSCug21145

  Symptom: When system crashes, sometimes core files are generated with CRC errors.

  Conditions: This issue occurs when the system crashes under stress conditions.

  Workaround: There is no workaround.

- CSCug22122

  Symptom: IOMD crash is seen for any IM on the router.

  Conditions: The IOMD crash is seen when show platform software agent IOMD 0/1 driver stats command is executed to verify driver statistics.

  Workaround: There is no workaround.

- CSCug23372

  Symptom: Manager process crash occurs while configuration replace operation is performed.

  Conditions: This issue occurs while moving from REP to G8032.

  Workaround: Avoid performing a configuration replace.

- CSCug26432

  Symptom: Egress layer3 multicast drops to few BDI outgoing interfaces after a router reload.

  Conditions: This issue occurs after router reload.

  Workaround: There is no workaround.

- CSCug31414

  Symptom: Multicast traffic drops on changing interface configuration from TEFP to VPLS over port channel (PoCH).

  Conditions: This issue occurs when converting a layer 2 interface to layer 3; and then configuring IP PIM and IP address in quick succession.

  Workaround: Use **shutdown** and **no shutdown** command on the interface.

- CSCug39899

  Symptom: Traffic stops flowing through QinQ BDI interface after ARP times out and ARP is removed by shutting the BDI.

  Conditions: This issue occurs when static routing is configured, and no routing protocol is configured on the interface.

  Workaround: Manually resolve the ARP by pinging the BDI interface.

- CSCug46010

  Symptom: The non IP packets get classified under the second class instead of class-default when two class-maps one having match on L4 ACL and other having match on L3 ACL with permit ip any any is configured.

  Conditions: This issue occurs when two class-maps one matching on L3 ACL match and another matching on TCP or UDP are configured.

  Workaround: There is no workaround.

- CSCug52920

  Symptom: EFP stats does not work after applying the QoS policy on the EFP.

  Conditions: This issue occurs when service policy is applied on the EFP.

  Workaround: There is no workaround.

- CSCug55586

  Symptom: If you dynamically remove the egress markings, ingress marking does not work.

  Conditions: This issue is observed if a marking is present at the logical level in the egress direction, DM does not work.

  Workaround: Use the egress set at leaf or PHB level.

- CSCug67955

  Symptom: The standby FP is stuck in init state.

  Conditions: This issue occurs after ISSU is performed.

  Workaround: There is no workaround.

- CSCug72785

  Symptom: OSPF flap observed on the router.

  Conditions: This issue occurs after IM OIR followed by SSO.

  Workaround: There is no workaround.

- CSCug73776

  Symptom: The standby router crashes on bootup when highly scaled configurations and when L2VPN and multicast are configured.

  Conditions: This issue occurs on reloading the router 3-4 times with highly scaled configurations and L2VPN and multicast are configured.

  Workaround: There is no workaround.

- CSCug83846

  Symptom: The MTU value does not take effect on an interface.

  Conditions: This issue is observed when you try to configure more than eight unique MTU values on the router.

  Workaround: There is no workaround.

- CSCug86963

  Symptom: Bidirectional Forwarding Detection (BFD) is unable to resolve neighbor Address Resolution Protocol (ARP).

  Conditions: This issue occurs when software BFD is configured with static client; and IM OIR or reload is performed.

  Workaround: Use manual ping.

- CSCug91295

  Symptom: UDP based ACLs do not work after a router reload.

  Conditions: This issue occurs after reload.

  Workaround: Remove and add the ACL.

- CSCug97639

  Symptom: IPv4 VRF ping fails when disabling IPv6 unicast-routing globally.

  Conditions: This issue occurs when IPv6 unicast-routing is disabled.

  Workaround: Enable IPv6 unicast-routing

- CSCuh16011

  Symptom: FMAN-FP crashes when you perform ab IM OIR.

  Conditions: This issue is observed when you perform multiple IM OIRs with around 65 BFD sessions.

  Workaround: Reload the router.

- CSCuh27117

  Symptom: Traffic loss of about six to eight seconds is observed when you perform an SSO.

  Conditions: This issue is observed when you perform the switchover before IM OIR or the interface flaps.

  Workaround: There is no workaround

- CSCuh77762

  Symptom: The TenGigabitEthernet port operates at one gigabit speeds in WAN-PHY mode on Cisco ASR 903 Routers. This leads to a huge amount of output drop.

  Conditions: This issue is observed if a QoS policy is configured on the TenGigabitEthernet interface.

  Workaround: There is no workaround.

- CSCuh86102

  Symptom: The interface stops forwarding traffic.

  Conditions: This issue is observed when the TenGigabitEthernet interface is in WAN-PHY mode and R0 is active.

  Workaround: Use R1

- CSCuh92939

  Symptom: Replacing the copper SFP with SFP causes traffic drop after SSO is performed

  Conditions: This issue occurs after replacing the copper SFP with the fiber SFP.

  Workaround: Perform an IM OIR.

- CSCuh94841

  Symptom: 10 Gigabit Ethernet interface flaps without trigger causing traffic to switch to protected label-switched path (LSP).

  Conditions: This issue occurs when the script is run for continuous SSO.

  Workaround: There is no workaround.

- CSCui08978

  Symptom: Crash observed on the router.

  Conditions: This issue occurs when shutdown followed by a no shutdown is performed on the physical interfaces.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.7(3)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.7(3)S.

- CSCuf89844

  Symptom: The router crashes when a bridge domain interface (BDI) interface running Bidirectional Forwarding Detection (BFD) is deleted.

  Conditions: This issue occurs when a static MAC address is assigned on the neighbor interface or on one of the BDI interface on the router and BDI interface running BFD is deleted.

  Workaround: There is no workaround.

- CSCug18630

  Symptom: CMAND process crash and tracebacks observed on the router.

  Conditions: This issue occurs after a hard OIR is performed and the standby RSP comes up.

  Workaround: There is no workaround.

- CSCuc42085

  Symptom: The 1PPS output from the router is out of range when compared to the 1PPS output of the PTP master clock.

  Conditions: This issue occurs when the router is configured as a hybrid clock (ordinary or boundary) and there are intermediate hops between the router and the PTP master clock. This issue occurs only when the intermediate hops are through an Cisco ASR 9000 router.

  Workaround: There is no workaround.

- CSCud34600

  Symptom: An event hog message is received when 21000 to 25000 routes are advertised into the Multiprotocol BGP (MBGP) and exported from one PE to other PE.

  Conditions: This issue occurs when the redistributing routes range from 21000 to 25000 routes from OSPF into MBGP and exported from a PE to other PE.

  Workaround: There is no workaround.

- CSCue77397

  Symptom: The Cisco ASR 903 manager crashes while flapping local MPLS enabled interfaces at nmpls_label_populate_flow_data.

  Conditions: This issue occurs when 6000 Layer3 VPN routes and 600 Layer2 VPN sessions exist.

  Workaround: There is no workaround.

- CSCuf85588

  Symptom: The pending objects from virtual forwarding interface (VFI) interfaces exists after shutdown of path when the core link comes up.

  Conditions: This issue exists when Ethernet over MPLS (EoMPLS) or VPLS with MPLS Tunnel TE in the core exists.

  Workaround: There is no workaround.

- CSCuf74113

  Symptom: Interface mode cannot be entered for serial interfaces.Error messages are displayed.

  Conditions: This issue occurs after creation of serial interfaces.

Workaround: There is no workaround.

- CSCud38115

  Symptom: OSPF connections flap and drop traffic for approximately 20 seconds

  Conditions: This issue occurs during stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCue07502

  Symptom: A crash is observed after completing ISSU. The F0/F1 are getting stuck in init state.

  Conditions: This issue occurs after completing ISSU.

  Workaround: Reload the router.

- CSCue24854

  Symptom: Performing an IM OIR in a remote LFA ring reports a loss of 70 ms.

  Conditions: This issue occurs during a soft OIR of the IM.

  Workaround: Perform a hard OIR for a loss less than 50 ms.

- CSCue87571

  Symptom: GLC-ZX-SM-RGD and GLC-LX-SM-RGD rapid SFP OIR causes ipprom to fail.

  Conditions: This issue occurs after rapid SFP OIR.

  Workaround: Perform each OIR with a delay of 30-40 seconds between the OIR. Reload the IM to recover the port.

- CSCuf07508

  Symptom: The Gigabit Ethernet port on interface module does not come up after a reload.

  Conditions: This issue occurs when the Cisco ASR 903 router is reloaded multiple times.

  Workaround: Perform an OIR of the interface module.

- CSCuf79397

  Symptom: The F1 interface is stuck in init state after OIR of the standby RSP or standby reload.

  Conditions: This issue occurs after the standby RSP is reloaded or OIR is performed.

  Workaround: There is no workaround.

- CSCub94462

  Symptom: The router displays object download error messages on the console similar to the following example:

  ```
  %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED"
  ```

  Conditions: Occurs when you take the following actions:

  - Apply the **mac address sticky** command
  - Configure 25 incremental MAC addresses
  - Apply the **clear mac-address-table bdomain** command
  - Remove a **mac security sticky** configuration from an EVC interface

  Workaround: Do not issue **clear mac-address-table** command when the **mac security sticky** is configured.

- CSCue51682

  Symptom: The REP protocol flaps, as indicated by the following error messages:

  ```
  *Feb  8 06:51:38.857: %REP-4-LINKSTATUS: GigabitEthernet0/0/1 (segment 10) is
  non-operational due to neighbor not responding
  *Feb  8 06:51:39.096: %REP-4-LINKSTATUS: GigabitEthernet0/0/1 (segment 10) is
  operational
  ```

  Conditions: Occurs under the following conditions:

  - The router is sending traffic using the incremental MAC address table
  - Fast LSL is configured using a 200ms timer.
  - The router is configured with more than 2000 MAC addresses.

  Workaround: Remove fast LSL from the REP configuration.

- CSCuf86247

  Symptom: SNMP MIB variables related to BDI counters do not function properly.

  Conditions: Occurs when you use SNMP MIB variables related to BDI interface counters.

  Workaround: There is no workaround.

- CSCug05491

  Symptom: The router drops traffic on VPLS circuits.

  Conditions: Occurs when you take the following actions:

  - Configure REP with VLAN load balancing
  - Configure VPLS VFI on the VLANs

  - Issue an stateful switchover (SSO)

  Workaround: There is no workaround.

- CSCuf86184

  Symptom: The **show interface BDI** command does not display the incrementing of counters when traffic is flowing.

  Conditions: This issue occurs after executing the **show interface BDI** command.

  Workaround: There is no workaround.

- CSCug30714

  Symptom: OSPF flaps occur on interface module stop.

  Conditions: This issue occurs when the interface module stops.

  Workaround: There is no workaround.

- CSCud96866

  Symptom: The router displays the following symptoms:

  - Object download failures
  - OSPF traffic flaps
  - High CPU utilization
  - Bundling and unbundling of port-channel member links
  - Slow console updates
  - Remote MEP learning failures

  Conditions: Occurs when you configure CFM offloaded MEPs for xconnect on a port-channel interface at a high scale and issue a **shutdown/no shutdow**n on the port-channel interface.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.7(3)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.7(3)S.

- CSCty30951

  Symptom: The router displays the following console error message: %QOSMGR-3-OUT_OF_TCAM_RESOURCES: SIP0: nile_mgr: Out of tcam resources to execute command

  Conditions: Occurs when you remove a QoS configuration by setting the interface to the default configuration.

  Workaround: There is no workaround.

- CSCty34054

  Symptom: The router displays CPU utilization traceback messages and drops all multicast traffic for 2050 seconds.

  Conditions: Occurs under the following conditions:

  - Multicast is enabled with more than 500 multicast groups.
  - The router is using RSP1B in SSM mode.
  - BDI is configured on the access side of the router.

- There are 24 EFPs on each bridge domain.
- You enter a **shutdown** command on the access interface.

Workaround: There is no workaround.

- CSCty74115

  Symptoms: The router displays traceback and CPU error messages.

  Conditions: Occurs when you configure a high number of MAC address table entries while REP is enabled; the router displays errors during a REP topology change, REP preemption, or when you perform a **shutdown/no shutdown** on an interface.

  Workaround: Reduce the number of MAC address entries.

- CSCua15499

  Symptoms: The **show interface** command output displays 1000 Mbps information for both 100Mbps and 10 gigabyte transceivers.

  Conditions: Occurs when you use 100 Mbps and 10 Gigabit Ethernet transceivers

  Workaround: There is no workaround.

- CSCua25779

  Symptom: An Ethernet virtual circuit (EVC) interface does not forward IPv4 traffic.

  Conditions: Occurs when you apply the **encapsulation dot1q** command to an EVC, followed by the **encapsulation untagged** command.

  Workaround: Issue a **shutdown/no shutdown** on the EVC interface.

- CSCua62305

  Symptom: QoS does not function on the router.

  Conditions: Occurs under the following conditions:

  - You apply a service-policy and an ACL to the same interface
  - You modify the ACL by adding an ACE containing a **permit ospf** statement.

  Workaround: There is no workaround.

- CSCub64331

  Symptom: The 10Mhz reference clock to the SDH Equipment Timing Source (SETS) goes to out-of-resource (OOR).

  Conditions: Occurs when you connect both 10Mhz and 1pps inputs.

  Workaround: Connect only the 10Mhz interface.

- CSCub71932

  Symptom: The OC-3 interface module (IM) crashes.

  Conditions: Occurs when you boot the router with an OC-3 IM and there are is no configuration applied to the IM. The issue occurs intermittently.

  Workaround: There is no workaround; wait for the interface module to reset.

- CSCub89531

  Symptom: Multicast statistics in the MFIB output can show NA/NA. This causes multicast traffic to drop every 3 minutes once the 3 minute timer expires.

  Conditions: Occurs after an stateful switchover (SSO).

  Workaround: Issue another SSO or reload the router.

- CSCuc43719

  Symptoms: The router crashes.

  Conditions: Occurs when you apply a Network Based Application Recognition (NBAR) configuration to the router. There is no specific trigger.

  Workaround: Remove the NBAR configuration, it is not supported.

- CSCuc55382

  Symptoms: The **show inventory** command displays incorrect serial number for SFPs and XFPs.

  Conditions: Occurs after you issue repeated stateful switchovers (SSOs).

  Workaround: There is no workaround.

- CSCuc59386

  Symptoms: Continuous IOMD crashes occur on OC-3 IM. Interfaces on OC-3 IM are not configurable and the router displays the the following error message:

  ```
  "stand-by does not support this command"
  ```

  Conditions: Occurs with OC-3 IM in a redundant configuration when an IOMD crash occurs on the active RSP and the standby IOMD session handle is not cleared.

  Workaround: Reload the standby RSP.

- CSCuc62784

  Symptoms: The router displays traceback error messages at niles_if_count_initialize

  Conditions: Occurs following a reload or stateful switchover (SSO).

  Workaround: There is no workaround. However, the issue does not have any functionality impact.

- CSCuc64654

  Symptom: The router is unable to ping the remote customer edge (CE) router.

  Conditions: Occurs when the router is acting as a provider edge (PE) device and is connected to the remote PE using dual loopback interfaces for peering with iBGP sessions.

  Workaround: Use a single loopback interface. Use the same loopback interface for IPv4 and VPNv4 address families.

- CSCuc66393

  Symptom: The router loses OC-3 interface configurations after an ISSU upgrade.

  Conditions: Occurs on OC-3 serial and POS interfaces after an ISSU software upgrade.

  Workaround: There is no workaround.

- CSCuc68462

  Symptom: The router drops PTP traffic.

  Conditions: The issue occurs occasionally when you configure PTP slave clock to receive VLAN-tagged traffic.

  Workaround: There is no workaround.

- CSCuc85721

  Symptom: The router crashes.

  Conditions: Occurs under the following conditions:

  – MR-APS is configured on serial interfaces on the OC-3 interface module

  - The router is configured with a high number of serial interfaces
  - You reset an interface module or reload the router.

  Workaround: There is no workaround.

- CSCuc91007

  Symptom: A slave clock displays a high 1PPS offset value from the master clock.

  Conditions: Occurs after an interface module reset or stateful switchover (SSO) on the master device.

  Workaround: There is no workaround.

- CSCuc95590

  Symptom: The router does not automatically upgrade the FPGA software.

  Conditions: Occurs when you load a new image while running an older FPGA version.

  Workaround: There is no workaround; however the issue has no functional impact.

- CSCuc98185

  Symptom: One out of 48 EFPs in a BDI does not receive traffic when running L3 multicast. The issue does not happen consistently.

  Conditions: Occurs under the following conditions:

  - You configure Protocol-Independent Multicast-Sparse Mode (PIM-SM) with a static rendezvous point (RP).
  - You configure a bridge domain interface (BDI) on the PE2 access side
  - You use the BDI to send IGMP v2 static join messages to a single multicast group
  - You disable IGMP snooping globally.
  - You configure 24 EFPs and map them to a single bridge-domain.
  - You initiate multicast traffic.
  - With multicast traffic enabled, you configure 24 EFPs and map them to the existing bridge-domain.

  One of the 48 EFPs does not receive traffic.

  Workaround: Reload the router.

- CSCud01644

  Symptom: The active forwarding processor (FP) is on the standby route switch processor (RSP).

  Conditions: Occurs when you boot the two RSPs in quick succession and the FP on the standby RSP becomes active before the FP on the active RSP.

  Workaround: Reload the router.

- CSCud07236

  Symptoms: The router displays console error messages when reloading.

  Conditions: Occurs when you reload the router.

  Workaround: There is no workaround; however, the messages have no impact on device.

- CSCud07642

  Symptom: The ASR 903 router is unable to pass traffic to the ASR 9000.

  Conditions: Occurs with a clear-channel ATM over MPLS configuration using AAL0 encapsulation.

  Workaround: Enable MPLS control-word on the ASR 9000.

- CSCud09632

  Symptom: The router does not correctly update the J0 byte on the OC-3 or OC-12 interface module.

  Conditions: Occurs in a back-to-back configuration with two ASR 903s passing SONET traffic.

  Workaround: There is no workaround.

- CSCud15785

  Symptom: The router experiences flapping on REP connections.

  Conditions: Occurs under the following conditions:

  - MAC limiting is enabled and a MAC address is at the maximum value
  - REP is configured with a 200 millisecond LSL ageout timer

  Workaround: Increase the REP timer to above 500 milliseconds or disable the MAC limiting feature.

- CSCud15841

  Symptom: The **clear ip mroute** * command causes resource leakage.

  Conditions: Occurs when you issue the **clear ip mroute** * command while IP multicast is enabled.

  Workaround: Reload the router.

- CSCud17457

  Symptom: The router drops IP multicast traffic.

  Conditions: Occurs when you perform the following actions:

  - Configure EFPs as members of a port channel containing a single interface.
  - Remove the configuration for the EFPs
  - Remove the interface from the port channel
  - Add the EFPs back onto the interface

  Workaround: Reload the router or issue a stateful switchover (SSO).

- CSCud23698

  Symptom: The router stops applying classification and marking for a class.

  Conditions: Occurs when you remove a priority level while using dual priority for the class-map.

  Workaround: Remove and reattach the policy-map on the interface.

- CSCud28982

  Symptom: The router does not process egress CoS marking on an Ethernet service instance.

  Conditions: Occurs when you configure QoS on an Ethernet service instance that is a member of a bridge-domain and uses dot1q encapsulation.

  Workaround: There is no workaround.

- CSCud30806

  Symptoms: The router accepts a QoS WRED configuration containing **match-all** configurations for two different **prec** values, which is not supported.

  Conditions: Occurs when you configure a policy with a class-map containing **match-all** configurations for two different **prec** values.

  Workaround: There is no workaround.

- CSCud33298

  Symptom: The router crashes.

  Conditions: Occurs when the peer device shuts down.

  Workaround: There is no workaround.

- CSCud34346

  Symptom: The router crashes.

  Conditions: The issue can occur when:

  – The router is configured with multiple ECMP paths

  – MPLS IP is not enabled on one of the ECMP paths

  Workaround: There is no workaround.

- CSCud35689

  Symptoms: The router accepts a queue-limit configuration at the parent level of a policy or at the Vlan class/ port level. This configuration is not supported.

  Conditions: Occurs when you add a queue-limit configuration on a policy at the parent level or at the vlan class/ port level.

  Workaround: There is no workaround.

- CSCud37927

  Symptoms: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs when the router is passing REP or STP traffic and one port is in an ALT or BLK state.

  Workaround: There is no workaround.

- CSCud38164

  Symptom: The router displays an object download failure message on the console.

  Conditions: Occurs when the number of ip routes reaches its maximum configurable limit.

  Workaround: There is no workaround.

- CSCud38433

  Symptom: The router is unable to establish MPLS neighborship or ping the destination loopback interface.

  Conditions: Occurs when you configure two Equal Cost Multipath (ECMP) paths on a bridge domain interface (BDI) using static routes.

  Workaround: The following workarounds exist:

  – Use Interior Gateway Protocol (IGP) instead of static IP routes.

  – Shut down one of the ECMP paths.

- CSCud40930

  Symptom: Some interfaces within a bridge-domain are unable to send outbound L3 multicast traffic.

  Conditions: Occurs when the bridge-domain contains EFP interfaces, some of which are on a port-channel. The issue can also occur after a router reload.

  Workaround: Issue a **shutdown/no shutdown** on the BDI interface.

- CSCud44768

  Symptom: Multilink bundles and member links flap when passing traffic.

  Conditions: Occurs under the following conditions:

  - You configure more than 210 MLPPP bundles with one member link per bundle or 16 bundles with 16 member links each.
  - The line is operating at a 64 or 128 byte line rate

  Workaround: There is no workaround.

- CSCud44942

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs when you configure a MEP on an interface.

  Workaround: There is no workaround.

- CSCud49980

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs when you configure CFM MEPs on carrier edge (CE) routers and VPLS on provider edge (PE) routers.

  Workaround: Create an EVC bridge-domain running CFM on the PE router and enable a virtual forwarding interface (VFI) on the bridge-domain.

- CSCud50851

  Symptom: The router experiences flapping on REP connections.

  Conditions: Occurs when you enable MAC limiting at a high scale and the set of MAC addresses changes continuously.

  Workaround: Disable MAC limiting.

- CSCud50944

  Symptom: The router drops traffic on an MLPPP bundle.

  Conditions: Occurs following a reload while the router is passing traffic close to the line rate. The issue occurs less frequently with lower traffic rates.

  Workaround: Issue a **shutdown/no shutdown** on multilink interface.

- CSCud55377

  Symptom: The router crashes.

  Conditions: Occurs when you configure offloaded CFM for xconnect sessions at a high scale.

  Workaround: There is no workaround.

- CSCud55695

  Symptom: The router applies the shaper value to the channel-level PIR for all serial interfaces on the interface module.

  Conditions: Occurs when you apply QoS policy with a port level class-default configuration containing a shaper value to a serial interface.

  Workaround: Add a dummy class-default level at the top of the policy and apply the shaper as a child policy of this class.

- CSCud56071

  Symptom: The router does not pass loop-free alternate (LFA) IP fast reroute (IPFRR) traffic.

  Conditions: Occurs when the router is configured with 10 or more IPv4 prefixes.

  Workaround: Configure 9 or fewer prefixes.

- CSCud61931

  Symptom: As OC-3 interface module controller does not become active using loopback local.

  Conditions: Occurs with the A900-IMA4OS interface module when there is no SFP inserted in the port.

  Workaround: Insert an SFP in the appropriate port.

- CSCud64034

  Symptoms: T1 interfaces do not become active.

  Conditions: Occurs when you perform the following actions:

  1. Configure T1 interfaces on the router.
  2. Use ping to verify that the interfaces are active
  3. Perform a stateful switchover (SSO)
  4. Use ping to verify that the interfaces are active
  5. Remove the T1 interface configuration
  6. Reload the standby RSP
  7. Reconfigure the T1 interfaces

  The T1 interfaces do not become active.

  Workaround: Perform an OIR on the interface module.

- CSCud64129

  Symptoms: The router displays CLI options to configure control-plane policing, which is not supported.

```
ASR903(config)#control-plane
ASR903(config-cp)#service-policy ?
input   Assign policy-map to the input of an interface
output  Assign policy-map to the output of an interface
```

  Conditions: Occurs when you attempt to configure control plane policing to restrict traffic punted by the CPU.

  Workaround: There is no workaround; the feature is not supported.

Further Problem Description: The ASR 903 has an implicit policer to restrict traffic destined for the CPU. The router polices this traffic up to 1Mbps by default, and this value is adjustable. For more detail, see http://www.cisco.com/en/US/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-punt-police-monitor.html

- CSCud65779

  Symptom: The router does not update the Rx value for C2, J1, and S1S0 bytes.

  Conditions: Occurs when you configure overhead bytes on OC-3 connections.

  Workaround: There is no workaround.

- CSCud71546

  Symptom: The ten Gigabit Ethernet interface drops traffic for 7 seconds following a stateful switchover (SSO).

  Conditions: Occurs when the configuration contains static routes to the destination.

  Workaround: There is no workaround.

- CSCud76209

  Symptom: The OC-3 interface module goes into an out of service state.

  Conditions: Occurs when you repeatedly perform an interface module reset (OIR) on the OC-3 interface module.

  Workaround: There is no workaround.

- CSCud76770

  Symptoms: The convergence time for FRR link/node protection is more than 2 seconds.

  Conditions: Occurs when you configure Next-Nexthop (NNHOP) backup tunnels in a ring topology.

  Workaround: There is no workaround.

- CSCud78168

  Symptoms: A higher convergence (>5 seconds) is observed for 3107 label imposition prefixes.

  Conditions: Occurs when you configure 3107 label imposition prefixes.

  Workaround: There is no workaround.

- CSCud83056

  Symptoms: PTP sessions remain in HOLDOVER mode.

  Conditions: Occurs when you remove and restore the PTP configuration on the PTP Master device.

  Workaround: Do not include the following commands in a PTP configuration unless ToD and 1PPS cables are directly connected:

  - **tod 0/0 ntp**
  - **input 1pps 0/0**

- CSCud83069

  Symptom: The router does not pass traffic in ATM PVP Mode.

  Conditions: Occurs when you enable ATM PVP Mode.

  Workaround: There is no workaround.

- CSCud83698

  Symptom: Links on the Gigabit Ethernet interface do not become active.

  Conditions: Occurs on the Gigabit Ethernet interface when the local interface is configured for autonegotiation and the remote interface is configured for a speed of 10 Mbps or 100 Mbps.

  Workaround: Toggle the auto-negotiation configuration on the Gigabit Ethernet interface.

- CSCud89451

  Symptom: The router crashes with an error message showing nmpls_label_populate_flow_data.

  Conditions: This issue occurs when the core interface is reset while the Cisco ASR 903 acts as a PE router running a configuration with Layer2 VPN and Layer3 VPN.

  Workaround: There is no workaround.

- CSCud90457

  Symptoms: The serial interface of Circuit Emulation interfaces connected to the CEM interfaces on PE remain down on router reload with scaled configuration.

  Conditions: This issue is observed when you have Circuit Emulation Services over Packet (CESoP) and Structure-agnostic TDM over Packet (SAToP) scaled circuits and perform a router reload.

  Workaround: Perform IM OIR to resolve the issue.

- CSCud90735

  Symptom: The controller comes up without having a license.

  Conditions: This issue occurs 16 port t1/e1 license are installed on PE1_W2

  Workaround: There is no workaround.

- CSCud90890

  Symptom: Routing over Trunk EFP over port-channel does not work on member ports associated with ASIC #1.

  Conditions: This issue occurs if a Trunk EFP on port-channel has members on ASIC #1.

  Workaround: There is no workaround.

- CSCud95359

  Symptom: The show policy map command displays an incorrect number of total dropped packets (total drops).

  Conditions: This issue occurs when the show policy-map command displays dropped packets on an interface.

  Workaround: There is no workaround.

- CSCud96604

  Symptoms: On system reset or reload, all traffic on certain Ethernet Flow Point (EFP)s do not egress.

  Conditions: This issue occurs when traffic completely stops on certain EFPs.

  Workaround: Delete and reconfigure EFPs.

- CSCud96962, CSCud97289

  Symptom: After performing a **shutdown** followed by a **noshutdown** the member-link Connectivity Fault Management (CFM) crash is observed

Conditions: This issue occurs when CFM Trunk Ethernet Flow Point (EFP) is configured with 256 sessions.

Workaround: Configure around 50-100 CFM sessions.

- CSCud97289

  Symptom: Precision Time Protocol (PTP) slave does not start the session with master.

  Conditions: This issue occurs when the PTP session is not started when the loopback IP address of slave and Master are in same subnet.

  Workaround: Configure Loopback IP addresses of slave and master in different subnets.

- CSCud99183

  Symptom: The control plane protocols such as ISIS, LDP do not come up and pings failure occurs on booting with scaled ACE or ACL. The ACL configurations fail.

  Conditions: This issue occurs on reload on the Cisco ASR 903 router.

  Workaround: There is no workaround.

- CSCud99692

  Symptom: The convergence time takes more than 3 seconds.

  Conditions: This issue occurs in Border Gateway Protocol (BGP) PIC core when path is moved from one active path to 2 Equal Cost Multipath (ECMP) Paths.

  Workaround: There is no workaround.

- CSCue00049

  Symptom: Classification does not work properly with non-matching traffic when IP ACL is used.

  Conditions: This issue occurs only for class-based ACL match. The ACL class are classified properly and other classes based on DSCP or class-default do not work

  Workaround: There is no workaround.

- CSCue00332

  Symptom: The Bidirectional Forwarding Detection (BFD) connections flap, bringing down IGP.

  Conditions: This issue occurs when you enable BFD on an interface that is flapping.

  Workaround: There is no workaround.

- CSCue03418

  Symptom: The router displays OSPF protocol flaps causing a 20-30 second traffic loss.

  Conditions: The issue occurs very intermittently on a HA system with a 6 second dead-interval value when you issue the redundancy force-switchover command;

  Workaround: Increase the dead-interval value.

- CSCue11444

  Symptom: Split horizon configurations does not clear with Layer2 multicast packets.

  Conditions: This issue occurs when Ethernet Flow Point (EFP)s with split-horizon are configured.

  Workaround: Perform a shutdown followed by no shutdown. Configure EFP first before moving into split-horizon group.

- CSCue16617

  Symptom: The QoS classification does not work in core interfaces.

  Conditions: This issue occurs when the output policy applied to interface has bridge domain interface (BDI) as the core interface.

  Workaround: Enable **mpls ldp explicit null** command.

- CSCue18015

  Symptom: S,G does not get created, the forwarding is based on (*,G).

  Conditions: This issue occurs with Interior Gateway Protocol (IGP) change leading to Reverse Path Forwarding (RPF) change of the (*,G).

  Workaround: Clear the (*,G) and recreate it.

- CSCue19898

  Symptom: (*,G) based forwarding is observed with IIF registry change. The Interior Gateway Protocol (IGP) patch change leads to this issue.

  Conditions: This issue occurs when IGP is changed causing a Reverse Path Forwarding (RFP) change notification.

  Workaround: Timeout the (*,G) entry and recreate it again either by issuing **clear ip mroute** command or stopping the joins.

- CSCue20022

  Symptom: Software forwarding of core encapsulation entries causes interface to flap.

  Conditions: This issue occurs when interface has Protocol Independent Multicast (PIM) enabled on the BDI interface.

  Workaround: Perform a soft interface module OIR. Clear the multicast routes for that VRF.

- CSCue20360

  Symptom: The router does not learn the remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: This issue occurs when Resilient Ethernet Protocol (REP) or Spanning Tree Protocol (STP) exists on core with one port as ALT or BLK state.

  Workaround: There is no workaround.

- CSCue20607

  Symptom: The port-channel load balances the traffic on member-links in hot-standby state or down state resulting in loss of traffic.

  Conditions: This issue occurs when there are redundant member-links in hot-standby state or down state.

  Workaround: There is no workaround.

- CSCue25567

  Symptom: Quack authentication failure messages are displayed on router console.

  Conditions: This issue occurs randomly.

  Workaround: Reload the router.

- CSCue26927

  Symptom: Alarms are not forwarded in Circuit Emulation Services over Packet (CESoP).

  Conditions: This issue occurs when alarms are not forwarded when AC goes down.

  Workaround: There is no workaround.

- CSCue30481

  Symptom: The Cisco ASR 903 router does not lock to the synchronous Ethernet clock source after reload. It remains in Ql-failed state.

  Conditions: This issue occurs after a reload of router with saved synchronous Ethernet clock configurations is performed.

  Workaround: Unconfigure and reconfigure the clock source.

- CSCue32753

  Symptom: The OC-3 interface modules are lost after a In Service Software Upgrade (ISSU) is performed on the Cisco ASR 903 router and configuration mismatch errors are displayed on router console. The standby RSP reaches standby-hot state causing continuous IOMD crash messages at regular intervals.

  Conditions: This issue occurs when ISSU is performed.

  Workaround: There is no workaround.

  Try unconfiguring the OC-3 interface module configuration and reconfigure again. Reload the standby RSP to stop IOMD crashes. Perform a hard OIR or process kill if the interface module enters out of service state

- CSCue34618

  Symptom: Traffic stops flowing with a combination of Bandwidth Remaining Ratio (BRR) and policer in different class-maps under a policy.

  Conditions: This issue occurs when the bandwidth remaining ratio is configured as a combination of police with cir (total brr and police cir equal to 1000M).

  Workaround: Configure total BRR and police cir lesser than 1000M. For example, class A Police cir 100m and class B BRR 90% fails but BRR 89% works.

- CSCue42315

  Symptom: CPU hog messages and IOMD crash observed on the Cisco ASR 903 router.

  Conditions: This issue occurs with OC-3 interface module after executing the **shutdown** command followed by a **no shutdown** command of the multilink bundle when traffic is sent with a packet size greater then 1500 byte.

  Workaround: There is no workaround.

- CSCue45498

  Symptom: CPU utilization is high when sending traffic with varying source MAC addresses for multiple streams for a bridge domain (BD).

  Conditions: This issue occurs when port-channel is configured as Ethernet Flow Point (EFP) for the BD and **mac-limit** is configured to 0 for that BD.

  Workaround: There is no workaround.

- CSCue50128

  Symptom: FMFP download failure occurs on reaching 1980 odd number even though 2000 ternary content addressable memory (TCAM) space is allocated for ACLs in the IP template.

  Conditions: This issue occurs in normal conditions when the scale reaches 1980.

  Workaround: There is no workaround.

- CSCue52298

  Symptom: TI/EI interfaces on interface module are lost as IOMD crashes after a switchover.

  Conditions: This issue occurs after IOMD crashes when a switchover was performed.

  Workaround: There is no workaround.

- CSCue52774

  Symptom: Sonet controller as input clock source does not get selected on A900-IMA4OS interface module on a Cisco ASR 903 router.

  Condition: This issue occurs when the port above 0 is used for the clock source.

  Workaround: Use port 0 for clock source or insert the SFP in the odd port (protect port) adjacent to the actual port using an optical splitter. The cable is fed to the odd port to recover the proper clocking for the port.

- CSCue52968

  Symptom: Ping failure occurs and traffic stops through Multilink bundle when Challenge Handshake Authentication Protocol (CHAP) authentication is enabled.

  Conditions: This issue is seen when Policy Feature Card (PFC) and Control Field Compression (ACFC) is configured on the Cisco ASR 903 router.

  Workaround: There is no workaround.

- CSCue57670

  Symptom: The active RSP synchronization LED displays the state incorrectly.

  Condition: This issue occurs after a Stateful Switchover (SSO) is performed without any network clock configuration.

  Workaround: There is no workaround. This issue is a cosmetic issue.

- CSCue59544

  Symptom: The A900-IMA16D generates a storm on closing the backup tunnel.

  Condition: This issue occur after unshutting the tunnel.

  Workaround: There is no workaround.

- CSCue66137

  Symptom: The IOMD crashes with CPU hog messages.

  Conditions: This issue occurs with OC-3 interface module and traffic is sent over a multilink bundle with packet size greater than 600 byte.

  Workaround: There is no workaround.

- CSCue72438

  Symptom: Link goes down with Rev-D I Gigabit interface module.

  Conditions: This issue occurs on the 1 Gigabit Ethernet interface module port.

  Workaround: There is no workaround.

- CSCue77612

  Symptom: MAC address synchronization on 1 Gigabit Ethernet port on standby RSP causes traffic to be forwarded to incorrect port after a switchover.

  Conditions: This issue occurs after a switchover.

  Workaround: Clear MAC address after a switchover is performed.

- CSCue86696

  Symptom: Interface flaps after longevity run is performed.

  Conditions: This issue occurs after prolonged tests are performed with SPF interface modules.

  Workaround: There is no workaround.

- CSCue87542

  Symptom: Deleting bridge domain interfaces (BDIs) with routing traffic causes a flood to CPU resulting in control plane traffic loss.

  Conditions: This issue occurs after a ping failure and the Bidirectional Forwarding Detection (BFD) protocol or OSFP protocol flaps on deleting the BDI while IPv4 traffic is flowing.

  Workaround: Delete the Trunk EFP interface and then the BDI.

- CSCue89503

  Symptom: The power supply status displays critical after removing and inserting the power supply on the Cisco ASR903 router.

  Conditions: This issue occurs after multiple OIR of the power supply is performed.

  Workaround: There is no workaround. This issue is cosmetic.

- CSCuf05039

  Symptom: I2C-WRITE and MDIO_READ error messages are displayed on the Cisco ASR903 router.

  Conditions: This issue occurs after an interface module hard or soft OIR is performed.

  Workaround: There is no workaround.

- CSCuf61365

  Symptom: Virtual circuit counters do not increment after interface module Online Insertion and Removal (OIR) followed by a SSO is performed.

  Conditions: This issue occurs after an OIR followed by a SSO is performed.

  Workaround: Perform a SSO without a interface module OIR.

- CSCuf65040

  Symptom: 1 Gigabit Ethernet or 10 Gigabit Ethernet interface module enters out of service state.

  Conditions: This issue occurs when a hard Online Insertion and Removal (OIR) is performed on the interface module.

  Workaround: Perform another hard OIR or a Stateful Switchover (SSO) followed by a soft OIR.

Open Caveats—Cisco IOS XE Release 3.7(2)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.7(2)S.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

  Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCty30951

  Symptom: The router displays the following console error message: %QOSMGR-3-OUT_OF_TCAM_RESOURCES: SIP0: nile_mgr: Out of tcam resources to execute command

  Conditions: Occurs when you remove a QoS configuration by setting the interface to the default configuration.

  Workaround: There is no workaround.

- CSCty34054

  Symptom: The router displays CPU utilization traceback messages and drops all multicast traffic for 2050 seconds.

  Conditions: Occurs under the following conditions:

  - Multicast is enabled with more than 500 multicast groups.
  - The router is using RSP1B in SSM mode.
  - BDI is configured on the access side of the router.
  - There are 24 EFPs on each bridge domain.
  - You enter a **shutdown** command on the access interface.

  Workaround: There is no workaround.

- CSCty76744

  Symptom: The **show mac-address-table** command does not show all of the EFPs with a given static MAC address; the command only displays the first EFP with the MAC address.

  Conditions: Occurs when you configure the same static MAC address on multiple EFPs.

  Workaround: There is no workaround; however, the issue is cosmetic and functionality is not affected.

- CSCua22323

  Symptom: Bit error rate testing (BERT) does not go in sync state.

  Conditions: Occurs when you configure BERT on the PDH controller in local loopback mode.

  Workaround: Initiate BERT on both ends of the connection.

- CSCua25779

  Symptom: An Ethernet virtual circuit (EVC) interface does not forward IPv4 traffic.

Conditions: Occurs when apply the **encapsulation dot1q** command to an EVC, followed by the **encapsulation untagged** command.

Workaround: Issue a **shutdown/no shutdown** on the EVC interface.

- CSCua35402

  Symptom: The router crashes.

  Conditions: Occurs under the following conditions:

  - The router is running static VPLS with 255 MPLS-TP tunnels and 2000 VCs.
  - The remote PE device reloads.

  Workaround: There is no workaround.

- CSCua57325

  Symptom: The router displays an OIR SPA error.

  Conditions: Occurs under the following conditions:

  - The router is running offloaded CFM sessions over an xconnect (pseudowire) interface.
  - The router is using a redundant hardware (dual RSP) configuration.
  - The remote router is using a non-redundant (single RSP) hardware configuration.
  - You reload the router.

  Workaround: There is no workaround.

- CSCua77688

  Symptom: The router experiences remote CFM MEP flapping.

  Conditions: Occurs when the router is connected via a CFM xconnect and the link is running a high traffic rate.

  Workaround: Reduce the rate of traffic.

- CSCua95675

  Symptom: An Ethernet virtual circuit (EVC) interface stops forwarding traffic.

  Conditions: Occurs when:

  - You configure multiple EVCs on a single interface
  - The EVCs have the same outer tag VLAN
  - You remove one of the EVCs from the configuration

  When you remove the EVC, other EVCs with the same outer tag VLAN can stop passing traffic.

  Workaround: Issue a **shutdown/no shutdown** on the Ethernet interface.

- CSCua99096

  Symptom: The **show ima interface** command omits some IMA group information such as ImaGroupSymmetry.

  Conditions: Occurs when you apply the **show ima interface** command.

  Workaround: There is no workaround.

- CSCub61344

  Symptom: Link Control Protocol (LCP) negotiation fails, causing an MLP bundle to stop passing traffic.

  Conditions: Occurs under the following conditions:

  - The router is configured with a T1 interface on the OC-3 interface module (IM)
  - The OC-3 interface module uses SONET framing
  - The T1 serial interface is part of an MLP bundle
  - You change the CRC configuration value of the MLP bundle

  Workaround: Follow these steps:

  - Remove the T1 interface from the MLP bundle.
  - Perform a soft OIR (IM reset) on both ends of the connection.
  - Wait for the T1 interface to become active.
  - Add the T1 interface back into the MLP bundle.

- CSCub63072

  Symptom: MPLS convergence can be slower than expected.

  Conditions: Occurs when the router switches to a backup MPLS path in the event of a network failure.

  Workaround: You can configure the following redundancy features to protect against network failures:

  - IPv4 Loop Free Alternate Fast Reroute (LFA FRR)
  - Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC)
  - MPLS Traffic Engineering (TE)--Fast Reroute (FRR) Link and Node Protection

- CSCub77354

  Symptom: An RSP switchover causes the serial interfaces to flap on the peer device.

  Conditions: Occurs when you perform an RSP switchover by physically removing the active RSP.

  Workaround: Use the following workarounds:

  - Perform an RSP switchover using the **redundancy force-switchover** command.

  Configure the local device to use **clock source line** and the remote device to use **clock source internal**.

- CSCub81445

  Symptom: A link remains active while the router shows the line protocol status as down.

  Link Stays up with Line Protocol status as down.

  Conditions: Occurs when you perform an interface module (IM) OIR, followed by a stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCuc38878

  Symptom: The router loops traffic between two nodes in a ring for approximately 100 ms.

  Conditions: Occurs during a failover when multiple ASR 903 routers are configured as nodes in a ring using Remote LFA FRR.

  Workaround: There is no workaround.

- CSCuc42085

  Symptom: The 1PPS output from the ASR 903 is out of range when compared to the 1PPS output of the PTP master clock.

Conditions: Occurs when the router is configured as a hybrid clock (ordinary/boundary) and there are intermediate hops between the router and the PTP master clock. To date the problem occurs only when the intermediate hops are through an ASR 9000 router.

Workaround: There is no workaround.

- CSCuc44701

  Symptom: The router displays an error message similar to the following: Oct 1 12:07:21.806 IST: %CMRP-3-CHASSIS_MONITOR_READY_TIME_EXCEEDED: R1/0: cmand: Reloading F1 because it has failed to become ready for packet processing

  Conditions: Occurs when you reload the router while running a configuration that contains

  - An egress QoS policy attached to a trunk EFP
  - An encapsulation dot1q statement within the QoS policy that specifies a large range

  Workaround: There is no workaround.

- CSCuc64654

  Symptom: The router is unable to ping the remote customer edge (CE) router.

  Conditions: Occurs when the router is acting as a provider edge (PE) device and is connected to the remote PE using dual loopback interfaces for peering with iBGP sessions.

  Workaround: Use a single loopback interface. Use the same loopback interface for IPv4 and VPNv4 address families.

- CSCuc68699

  Symptom: The router displays a segmentation fault error message at cgmu_nq_ccm_convert and crashes.

  Conditions: Occurs when you:

  - Remove QoS policy from an EFP interface
  - Remove policy-maps and class-maps from the configuration

  Workaround: There is no workaround.

- CSCuc83088

  Symptom: The router drops traffic during stateful switchover (SSO).

  Conditions: Occurs when the router is running HSRP or VRRP; the issue only occurs when the destination MAC address is a virtual MAC (vMAC) address.

  Workaround: Change the traffic priority and detour traffic prior to the SSO.

- CSCuc88066

  Symptom: The router does not classify egress traffic and the **show policy-map interface** command counters do not increment.

  Conditions: Occurs when you configure an output QoS policy to an EFP interface.

  Workaround: Remove and reconfigure the service policy on the EFP interface.

- CSCuc92350

  Symptom: A connection between two copper SFPs does not become active.

  Conditions: Occurs when two SFP interfaces are connected with one side set to 100 Mbps and the other side set to **negotiation auto**.

  Workaround: Set the speed to 10Mbps at both sides, then configure negotiation auto on one side of the connection.

- CSCuc99908

  Symptom: IEEE 802.1S Multiple STP (MSTP) convergence takes more than 4.1 seconds.

  Conditions: Occurs under the following conditions:

  - An Ethernet interface is acting as the Root forwarding MST port
  - The Ethernet interface is configured with more than 1000 EVCs
  - You perform a **shutdown/no shutdown** on the interface.

  Workaround: To achieve a convergence time of approximately 900 milliseconds with 1000 VLANs on an Ethernet interface, configure MSTP on a trunk EFP.

- CSCud01908

  Symptom: Debug commands show pending objects on the Forwarding Manager (FMAN) on the forwarding processor (FP), indicating a failure to download configurations from the Route Switch Processor (RSP) to the data plane (DP).

  Conditions: Occurs when you apply a QoS shaping configuration at a high scale.

  Workaround: Delete the QoS policies and remove the QoS configuration from the interface.

- CSCud04529

  Symptom: The router can drop traffic for approximately 300 milliseconds.

  Conditions: The issue occurs in rare instances when the router is configured in a ring topology with loop-free alternate (LFA) IP fast reroute (IPFRR) and the primary path recovers from a down state.

  Workaround: There is no workaround.

- CSCud07642

  Symptom: The ASR 903 is unable to pass traffic to the ASR 9000.

  Conditions: Occurs with a clear-channel ATM over MPLS configuration using AAL0 encapsulation.

  Workaround: Enable MPLS control-word on the ASR 9000.

- CSCud11843

  Symptom: The router displays a CPU hog error message and crashes.

  Conditions: Occurs when you issue an RSP switchover following an interface flap on the 10 Gigabit Ethernet interface module (IM).

  Workaround: The issue does not occur in the absence of in interface flap on the 10 Gigabit Ethernet IM.

- CSCud15785

  Symptom: The router experiences flapping on REP connections.

  Conditions: Occurs under the following conditions:

  - MAC limiting is enabled and a MAC address is at the maximum value
  - REP is configured with a 200 millisecond LSL ageout timer

  Workaround: Increase the REP timer to above 500 milliseconds or disable the MAC limiting feature.

- CSCud19845

  Symptom: The router drops ping packets over VPN Routing and Forwarding (VRF) connections.

  Conditions: Occurs when you specify a packet size using the **size** parameter.

Workaround: There is no workaround; however, the issue does not occur when you omit the **size** parameter.

- CSCud23647

  Symptom: BDI adjacency fails on the standby RSP.

  Conditions: The issue can occur during an interface module (IM) reset or router reload.

  Workaround: There is no workaround.

- CSCud24704

  Symptom: The router crashes.

  Conditions: Occurs when you perform an interface module OIR (reset) on the gigabit Ethernet interface module while the standby RSP is booting.

  Workaround: Perform the IM OIR after the standby RSP boots.

- CSCud26379

  Symptom: The router displays a CWAN OIR Handler traceback error.

  Conditions: Occurs when you perform an interface module OIR (reset) on the gigabit Ethernet interface module, followed by an RSP switchover.

  Workaround: Complete the RSP switchover without resetting the gigabit Ethernet IM.

- CSCud26812

  Symptom: The router CLI does not display some SFP PIDs

  Conditions: Occurs when you install one of the following SFPs in the router:

  - ONS-SI-155-L2
  - ONS-SI-155-L1
  - ONS-SI-155-I1

  Workaround: There is no workaround.

- CSCud28787

  Symptom: The 10 gigabit Ethernet interface module (IM) (IM- A900-IMA1X) flaps.

  Conditions: Occurs when the IM passes high traffic volumes for an extended period of time.

  Workaround: There is no workaround.

- CSCud28982

  Symptom: The router does not process egress CoS marking on an Ethernet service instance.

  Conditions: Occurs when you configure QoS on an Ethernet service instance that is a member of a bridge-domain and uses dot1q encapsulation.

  Workaround: There is no workaround.

- CSCud29501

  Symptom: The **show policy-map** command displays an incorrect drop rate value.

  Conditions: Occurs when you configuring a policy map that contains a class that applies QoS policing.

  Workaround: There is no workaround; however, the issue has no functional impact. The router displays the correct number of drops under the policer's exceeded bps value.

- CSCud33329

Symptom: The active RSP displays traceback error messages occurring on the standby RSP.

Conditions: Occurs with the following configuration:

- The router is configured with 1000 multicast groups
- The outgoing interface is a bridge-domain interface (BDI)
- All hosts are receiving a high rate of traffic.

The issue occurs after you issue a stateful switchover (SSO).

Workaround: Avoid performing an SSO with the configuration described.

- CSCud33906

  Symptom: Equal Cost Multipath (ECMP) loopback does not function properly.

  Conditions: Occurs when a port-channel link dynamically assigned as an ECMP path.

  Workaround: There is no workaround.

- CSCud34346

  Symptom: The router crashes.

  Conditions: The issue can occur when:

  - The router is configured with multiple ECMP paths
  - MPLS IP is not enabled on one of the ECMP paths

  Workaround: There is no workaround.

- CSCud38038

  Symptom: The router records incorrect delay measurements after a reload.

  Conditions: Occurs under the following conditions:

  - You configure Delay Measurement Message (DMM) on a port-channel interface.
  - The port-channel member links are on different interface modules (IMs).
  - You reload the router.

  Workaround: You can use the following workarounds:

  - Remove the **ethernet cfm global** command and re-apply it after the port-channel member links recover.
  - Configure PTP clock synchronization.

- CSCud38115

  Symptom: OSPF connections flap and drop traffic for approximately 20 seconds

  Conditions: Occurs during stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCud38419

  Symptom: The router crashes when you apply an access control list (ACL) configuration. The issue occurs rarely and when the router is configured at a high scale.

  Conditions: Occurs when:

  - You create and apply IPv6 ACLs
  - You remove the IPv6 ACLs
  - You replace the IPv6 ACLs with IPv4 ACLs

  - The IPv6 ACLs and IPv4 ACLs have the same names

  Workaround: Create IPv4 ACLs with different names from the IPv6 ACLs.

- CSCud38433

  Symptom: The router is unable to establish MPLS neighborship or ping the destination loopback interface.

  Conditions: Occurs when you configure two Equal Cost Multipath (ECMP) paths on a bridge domain interface (BDI) using static routes.

  Workaround: The following workarounds exist:

  - Use Interior Gateway Protocol (IGP) instead of static IP routes.
  - Shut down one of the ECMP paths.

- CSCud40930

  Symptom: Some interfaces within a bridge-domain are unable to send outbound L3 multicast traffic.

  Conditions: Occurs when the bridge-domain contains EFP interfaces, some of which are on a port-channel. The issue can also occur after a router reload.

  Workaround: Issue a **shutdown/no shutdown** on the BDI interface.

- CSCud44768

  Symptom: Multilink bundles and member links flap when passing traffic.

  Conditions: Occurs under the following conditions:

  - You configure more than 210 MLPPP bundles with one member link per bundle or 16 bundles with 16 member links each.
  - The line is operating at a 64 or 128 byte line rate

  Workaround: There is no workaround.

- CSCud44942

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs when you configure a MEP on an interface.

  Workaround: There is no workaround.

- CSCud45336

  Symptom: The router displays CPU hog error messages and crashes.

  Conditions: Occurs when you reload the router a high number of Structure-agnostic TDM over Packet (SAToP) pseudowires.

  Workaround: There is no workaround.

- CSCud49749

  Symptom: Copper Ethernet interface module (IM) ports remain in a suspended state after stateful switchover (SSO).

  Conditions: Occurs when you create a port-channel with

  - Two links from a copper Ethernet interface to another copper Ethernet interface
  - One link from a copper Ethernet interface to an SFP Ethernet interface

  Workaround: Issue a **shutdown/no shutdown** on copper-to-copper connection interfaces.

- CSCud49980

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs when you configure CFM MEPs on carrier edge (CE) routers and VPLS on provider edge (PE) routers.

  Workaround: Create an EVC bridge-domain running CFM on the PE router and enable a virtual forwarding interface (VFI) on the bridge-domain.

- CSCud50851

  Symptom: The router experiences flapping on REP connections.

  Conditions: Occurs when you enable MAC limiting at a high scale and the set of MAC addresses changes continuously.

  Workaround: Disable MAC limiting.

- CSCud50944

  Symptom: The router drops traffic on an MLPPP bundle.

  Conditions: Occurs following a reload while the router is passing traffic close to the line rate. The issue occurs less frequently with lower traffic rates.

  Workaround: Issue a **shutdown/no shutdown** on multilink interface.

- CSCud52920

  Symptom: SFP interfaces tied to a port-channel flap.

  Conditions: The issue occurs rarely when the router is passing a high traffic volume.

  Workaround: There is no workaround.

- CSCud56071

  Symptom: The router does not pass loop-free alternate (LFA) IP fast reroute (IPFRR) traffic.

  Conditions: Occurs when the router is configured with 10 or more IPv4 prefixes.

  Workaround: Configure 9 or fewer prefixes.

Resolved Caveats—Cisco IOS XE Release 3.7(2)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.7(2)S.

- CSCua62029

  Symptom: The router crashes.

  Conditions: Occurs when you configure a class-based QoS policy with the following characteristics:

  - The policy is attached to the main interface.
  - The policy classifies on multiple VLANs.
  - The classification statements specify a priority.
  - The classification statements are within a child QoS policy.

  Workaround: There is no workaround.

- CSCua73104

Symptoms: The router does not increment QoS port shaper policy counters displayed by the **show policy interface** command.

Conditions: Occurs when you configure -A class-default policy on a physical interface -A class-based policy on an EVC interface

Workaround: There is no workaround; however, the router applies the QoS policy normally.

- CSCua96186

  Symptom: The router drops cells on a CE-to-CE connection.

  Conditions: Occurs with ATM VCC and VPC cell relay mode with 64-byte traffic. The issue occurs between the ASR 903 and ASR 901 routers.

  Workaround: There is no workaround.

- CSCub69132

  Symptom: The OC-3 interface module crashes.

  Conditions: Occurs when you issue a soft reload on the OC-3 interface module when the

  router is configured with MLPPP at a high scale.

  Workaround: There is no workaround.

- CSCuc36056

  Symptom: Security ACLs with port ranges configured on BDI interfaces will not work on NILE1 ports.

  Conditions: Issue with only on NILE1 ports. NILE0 ports will work properly

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C CVE ID CVE-2012-5716 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc44394

  Symptom: The router stops passing MLPPP traffic after a Stateful Switchover (SSO).

  Conditions: Occurs when you perform an SSO with a TDM interface module.

  Workaround: There is no workaround.

- CSCuc57130

  Symptom: The router does not apply OC-3 interface module (IM) configurations.

  Conditions: Occurs after an RSP switchover.

  Workaround: There is no workaround.

- CSCuc64899

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs on interfaces with an xconnect statement after a reload on a peer device.

  Workaround: Remove and re-apply the CFM configuration.

- CSCuc80964

Symptom: Interface module (IM) IM FPGA upgrade fails.

Conditions: Occurs on some IMs when you install an IOS image with bundled FPGA software.

Workaround: Manually upgrade the FPGA.

- CSCuc98590

  Symptom: The router can crash when you remove a boundary clock (BC) configuration.

  Conditions: Occurs very rarely when you remove a BC configuration.

  Workaround: There is no workaround. However, the issue occurs very rarely.

- CSCud12587

  Symptom: When handling IS-IS packets, the router punts the traffic to the Route Switch Processor (RSP) and applies policing to limit the traffic to 1 Mbps.

  Conditions: Occurs when you enable IS-IS over an Ethernet over MPLS (EoMPLS) connection.

  Workaround: Use IS-IS over another connection type or limit the IS-IS traffic to less than 1 Mbps.

- CSCud13535

  Symptom: The router drops imposition traffic sent to a neighbor device over a VPLS pseudowire.

  Conditions: Occurs when the neighbor device configuration includes the **no split horizon group** command.

  Workaround: Remove the **no split horizon group** command from the VPLS neighbor device.

- CSCud28787

  Symptom: The 10 gigabit Ethernet interface module (IM) flaps.

  Conditions: Occurs when the IM passes high traffic volumes for an extended period of time.

  Workaround: There is no workaround.

- CSCud43580

  Symptom: The router does not apply the **bandwidth remaining percent** command within a QoS policy in some instances.

  Conditions: The issue can occur occasionally when:

  - There is a large discrepancy in **bandwidth remaining** values between QoS classes
  - The classes containing the **bandwidth remaining** statements are oversubscribed at a low rate or have a low queue-limit.

  Workaround: Apply the following workaround:

  - Increase the **queue-limit** value to 120 kilobytes or above.
  - If the QoS configuration uses WRED, increase the minimum threshold value.
  - Alter the bandwidth remaining values to reduce the ratio between values.

Open Caveats—Cisco IOS XE Release 3.7(1)aS

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.7(1)aS.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCtw76473

  Symptom: The router displays packet drops on some VPLS pseudowire virtual circuits (VCs) on the disposition side.

  Conditions: Occurs under the following conditions:

  - The core network is running MPLS-TP tunnels
  - There is an SSO switchover on the remote end or an LDP neighbor reset on the peer end.

  Workaround: There is no workaround.

- CSCty34054

  Symptom: The router displays CPU utilization traceback messages and drops all multicast traffic for 2050 seconds.

  Conditions: Occurs under the following conditions:

  - Multicast is enabled with more than 500 multicast groups.
  - The router is using RSP1B in SSM mode.
  - BDI is configured on the access side of the router.
  - There are 24 EFPs on each bridge domain.
  - You enter a **shutdown** command on the access interface.

  Workaround: There is no workaround.

- CSCty45696

  Symptom: The **show policy-map** command displays incorrect information.

  Conditions: Occurs when you use the **show policy-map** command to display QoS policies on an EFP that has a port shaping QoS policy.

  Workaround: There is no workaround.

- CSCtz55979

  Symptom: The router crashes.

  Conditions: Occurs when you configure CFM, SCE over MPLS, VPLS, or G.8032 services while running SNMP polling.

  Workaround: There is no workaround.

- CSCtz68510

  Symptom: The router displays a CPU HOG message.

  Conditions: Occurs when you remove a PTP configuration.

  Workaround: There is no workaround; however, the issue does not have any functionality impact.

- CSCua62029

  Symptom: The router crashes.

  Conditions: Occurs when you configure a class-based QoS policy with the following characteristics:

- The policy is attached to the main interface.
- The policy classifies on multiple VLANs.
- The classification statements specify a priority.
- The classification statements are within a child QoS policy.

Workaround: There is no workaround.

- CSCua96186

  Symptom: The router drops cells on a CE-to-CE connection.

  Conditions: Occurs with ATM VCC and VPC cell relay mode with 64-byte traffic. The issue occurs between the ASR 903 and ASR 901 routers.

  Workaround: There is no workaround.

- CSCub04699

  Symptom: The **bandwidth** and **bandwidth percent** commands do not function correctly.

  Conditions: Occurs when you configure a service-policy with the **priority** and **police** commands in one class and the **bandwidth** or **bandwidth percent** commands in another class.

  Workaround: There is no workaround.

- CSCub48081

  Symptom: The router does not learn remote MEPs on an EVC bridge-domain MEP following an interface module reset (soft OIR). The router displays messages indicating object download failure; the interface status of the xconnect MEP on the peer router displays as administratively down.

  Conditions: Occurs when you

  - Configure offloaded EVC xconnect MEP sessions and the sessions are active
  - Configure EVC bridge-domain MEPs
  - Perform a reset (soft OIR) of the Ethernet interface module

  Workaround: Remove and restore the local MEP configuration on both routers.

- CSCub55760

  Symptom: The router displays a Delay Measurement Message (DMM) delay value of 0.

  Conditions: Occurs under the following conditions:

  - You configure an EVC down MEP on a port-channel interface.
  - You dynamically add a member link to a port-channel interface.

  Workaround: Configure PTP synchronization before scheduling DMM.

- CSCub60668

  Symptom: The router is unable to establish an OSPF session.

  Conditions: Occurs when you enable an OSPF session over an MPLS TP tunnel.

  Workaround: There is no workaround.

- CSCub69132

  Symptom: The OC-3 interface module crashes.

  Conditions: Occurs when you issue a soft reload on the OC-3 interface module when the router is configured with MLPPP at a high scale.

  Workaround: There is no workaround.

- CSCub78861

  Symptom: Following a reload, the router handles CFM only on 128 VLANs or bridge-domains.

  Conditions: Occurs when the router configuration contains CFM and more than 128 VLANs or bridge-domains.

  Workaround: There is no workaround.

- CSCuc00986

  Symptom: The router drops MPLS TP sessions, impacting traffic.

  Conditions: Occurs following an software upgrade (ISSU).

  Workaround: There is no workaround.

- CSCuc23610

  Symptom: The router does not pass IP traffic with an MPLS LDP tunnel label of Imp-null.

  Conditions: Occurs when the router is switching traffic using IP fast-reroute (FRR).

  Workaround: Configure the **mpls ldp explicit-null** command.

- CSCuc31037

  Symptom: The router stops passing traffic on pseudowire connections.

  Conditions: Occurs in a redundant system following a stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCuc34088

  Symptom: The router passes lower traffic levels when you add links to an IMA bundle and perform IM OIR/router reload.

  Conditions: Occurs when you send traffic above the E1 line rate on one link within an IMA bundle and reset (OIR) the interface module.

  Workaround: Remove and re-apply the IMA interface configuration.

- CSCuc36522

  Symptom: The router does not timestamp traffic on port-channel interfaces.

  Conditions: Occurs when you configure a CFM EVC bridge-domain up MEP on a port-channel.

  Workaround: There is no workaround.

- CSCuc42085

  Symptom: The 1PPS output from the ASR 903 is out of range when compared to the 1PPS output of the PTP master clock.

  Conditions: Occurs when the router is configured as a hybrid clock (ordinary/boundary) and there are intermediate hops between the router and the PTP master clock. To date the problem occurs only when the intermediate hops are through an ASR 9000 router.

  Workaround: There is no workaround.

- CSCuc42206

  Symptom: Links on copper SFP interface flap during stateful switchover (SSO).

  Conditions: Occurs when you initiate a stateful switchover (SSO) on a redundant system with a copper SFP.

  Workaround: There is no workaround.

- CSCuc44394

  Symptom: The router stops passing MLPPP traffic after a Stateful Switchover (SSO).

  Conditions: Occurs when you perform an SSO with a TDM interface module.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.7(1)aS

This section documents the issues that have been resolved in Cisco IOS XE Release 3.7(1)aS.

- CSCty63969

  Symptoms: Ping fails to remote MEPs.

  Conditions: Occurs when you configure CFM and ping RMEPs with a packet size of greater than 1478 bytes.

  Workaround: There is no workaround.

- CSCua02058

  Symptoms: When you configure the OC-3 interface module, only 1000 of 1008 interfaces are configurable on the router; of the 1000 interfaces, only 957 become active.

  Conditions: Occurs when you configure interfaces on the OC-3 interface module.

  Workaround: There is no workaround.

- CSCua51772

  Symptoms: The router does not display PID or DOM values.

  Conditions: Occurs with the following SFPs:

  - ONS-SI-155-L2
  - ONS-SI-155-L1
  - ONS-SI-155-I1

  Workaround: There is no workaround.

- CSCua55122

  Symptoms: The OC-3 interface module crashes when you create a high number of ATM IMA interfaces.

  Conditions: Occurs when you configure multiple ATM IMA interfaces with fewer than 16 links per bundle.

  Workaround: Perform a hard OIR on the interface module.

- CSCua87805

  Symptoms: The OC-3 interface module goes into an Out Of Service state.

  Conditions: The issue can occur during bootup or OIR of the OC-3 interface module.

  Workaround: Perform an OIR on the OC-3 interface module.

- CSCua93803

  Symptoms: The **boot system flash** command displays unexpected behavior.

  Conditions: Occurs when you use the **boot system flash** command in either of the following formats:

  - **boot system flash** *filename*—The router does not boot using the specified file.
  - **boot system flash**—The router does not boot the first image in bootflash.

  Workaround: Use the **boot system bootflash** command as follows:

  - **boot system bootflash:** *filename*—Boots a specific file.
  - **boot system bootflash:**—Boots the first image in bootflash.

- CSCua95522

  Symptoms: The router displays the following warning during bootup:

  ```
  "Warning: monitor nvram area is corrupt ... using default values"
  ```

  Conditions: Occurs during bootup and indicates that the NVRAM is corrupted, causing loss of a bootloader variable. To verify the issue, confirm whether the **set** rommon mode command produces output matching the following example:

  ```
  rommon 1 > set
  PS1=rommon ! >
  rommon 2 >
  ```

  The issue can be caused by an error during shutdown or saving the configuration and occurs very rarely.

  Workaround: Set the bootloader variables on the standby RSP.

- CSCua99096

  Symptoms: The **show ima interface** command omits some IMA group information such as ImaGroupSymmetry.

  Conditions: Occurs when you apply the **show ima interface** command.

  Workaround: There is no workaround.

- CSCua99096

  Symptoms: The **show ima interface** command omits some IMA group information such as ImaGroupSymmetry.

  Conditions: Occurs when you apply the **show ima interface** command.

  Workaround: There is no workaround.

- CSCub04699

  Symptom: The **bandwidth** and **bandwidth percent** commands do not function correctly.

  Conditions: Occurs when you configure a service-policy with the **priority** and **police** commands in one class and the **bandwidth** or **bandwidth percent** commands in another class.

  Workaround: There is no workaround.

- CSCub55266

  Symptoms: The router hangs when booting.

  Conditions: Occurs under the following conditions:

  - You issue the boot command without any arguments, e.g. `rommon 1> boot`
  - The router attempts to boot using a non-bootable image in bootflash memory.

  Workaround: There is no workaround.

- CSCub71578

  Symptoms: The router displays traceback and failure messages on the standby RSP.

Conditions: Occurs after you issue an OIR on the T1/E1 interface module from the active RSP. The issue occurs in a redundant system.

Workaround: There is no workaround.

- CSCub74338

  Symptoms: The router crashes.

  Conditions: Occurs when you attach an ingress QoS policy-map to an EVC with a rewrite push configuration.

  Workaround: There is no workaround.

- CSCub77285

  Symptom: Some T1/E1 interfaces do not come up.

  Conditions: Occurs with T1/E1 configurations at a high scale; the interfaces display a false alarm.

  Workaround: Reset individual T1/E1 interfaces; after a reset, the interfaces become active.

- CSCub89029

  Symptoms: When the router boots, copper Gigabit Ethernet ports display an up/up status but do not pass traffic.

  Conditions: Occurs when the port has a negotiated speed other than 1 Gigabit, such as 100 Mbps.

  Workaround: Issue a shutdown/no shutdown on affected ports.

- CSCuc36241

  Symptoms: The router is unable to select a given PTP clock as a network clock source.

  Conditions: Occurs when you configure PTP as an input network clock source while the slave clock is still in a holdover state. In the holdover state, the slave clock has not yet attempted to establish a frequency lock with a master clock.

  Workaround: Wait for the PTP slave clock to lock to the master clock before configuring PTP as a network clock input source.

Open Caveats—Cisco IOS XE Release 3.7(0)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.7.0S.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

  Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCtw72855

  Symptoms: The router does not pass traffic towards the access side on VCs configured with QoS shaping output policy.

  Conditions: Occurs when you configure a QoS shaping output policy.

  Workaround: There is no workaround.

- CSCty28986

  Symptoms: A configuration with a high number of down MEPs does not function properly.

  Conditions: Occurs when you configure 500 or more down MEPs with 500 or more xconnect configurations between service instances.

  Workaround: Configure no more than 200 CFM sessions.

- CSCty34054

  Symptoms: The router displays CPU utilization traceback messages and drops all multicast traffic for 2050 seconds.

  Conditions: Occurs under the following conditions:

  - Multicast is enabled with more than 500 multicast groups
  - The router is using RSP1B in SSM mode
  - BDI is configured on the access side of the router
  - There are 24 EFPs on each bridge domain
  - You enter a **shutdown** command on the access interface.

  Workaround: There is no workaround.

- CSCty51990

  Symptoms: The router may crash or restart; the console displays a SW_WDOG: expired message.

  Conditions: Occurs under the following conditions:

  - The router is configured with 63 or more instances of a unique EVC configured with a unique bridge domain interface (BDI).
  - The router is sending IGMP joins to one multicast group.
  - You perform a shutdown/no shutdown on the interface sending IGMP join messages.
  - You perform an OIR on the router.

  Workaround: There is no workaround.

- CSCty70119

  Symptoms: Port shaper rate changes do not take effect.

  Conditions: Occurs when QoS policies attached to EVCs on an interface do not include a shaper configuration; the issue does not occur on EFP policies that include a shaper in a class.

  Workaround: Include a shaper in one class of the EFP policy.

- CSCty73362

  Symptoms: The router experiences CPP download failures when sending IGMP join messages.

  Conditions: Occurs when the router is configured with a trunk EFP in SM mode on the access side and is sending IGMP join messages to more than 1970 multicast groups.

  Workaround: There is no workaround.

- CSCty74115

  Symptoms: The router displays traceback and CPU error messages.

  Conditions: Occurs when you configure a high number of MAC address table entries while REP is enabled; the router displays errors during a REP topology change, REP preemption, or when you perform a shutdown/no shutdown on an interface.

  Workaround: Reduce the MAC scale.

- CSCty79987

  Symptoms: CFM up and down MEPs do not reach a scale of 1000 CFM sessions.

  Conditions: Occurs when you configure CFM on a trunk EFP.

  Workaround: There is no workaround.

- CSCtz20087

  Symptoms: The router applies the class-default QoS policy to all outgoing traffic.

  Conditions: Occurs under the following conditions:

  – You configure multiple egress QoS policies on a Gigabit Ethernet interface.

  – You configure a multilink interface with no ingress QoS policy

  Workaround: There is no workaround.

- CSCtz32327

  Symptoms: The router crashes.

  Conditions: Occurs when you perform an OIR on the OC-3 IM after an SSO switchover.

  Workaround: There is no workaround.

- CSCtz40690

  Symptoms: Traceroute to a remote MEP fails.

  Conditions: Occurs under the following conditions:

  – You configure a EVC bridge-domain MEP on a remote device

  – You configure a MIP on a trunk EFP on an intermediate device.

  – You issue the **traceroute** command to the remote MEP

  Workaround: There is no workaround.

- CSCtz49927

  Symptoms: Traffic floods on an EFP interface.

  Conditions: Occurs when you configure a multicast static MAC on a bridge-domain and add more than 24 EFPs.

  Workaround: Remove the extra EFPs from the bridge-domain.

- CSCtz55979

  Symptoms: The router crashes.

  Conditions: Occurs when you configure CFM, SCE over MPLS, VPLS, or G.8032 services while running SNMP polling.

  Workaround: There is no workaround.

- CSCtz75641

  Symptoms: The router does not pass traffic over an EVC PC port-channel.

  Conditions: Occurs when you perform the following sequence of actions:

  – Remove an EVC member link from a port-channel interface

  – Configure a trunk EFP -Set the interface to default

  – Add the EVC member link back into the port-channel interface

  Workaround: Reload the router.

- CSCtz77491

  Symptoms: The router stops passing traffic and crashes.

  Conditions: Occurs when you remove a QoS policy applied to a trunk EFP.

  Workaround: There is no workaround.

- CSCtz82725

  Symptoms: The router intermittently drops packets.

  Conditions: Occurs on 10 Gigabit Ethernet core links when the router passes traffic for an extended period and running a VPLS-TP configuration.

  Workaround: There is no workaround.

- CSCtz87262

  Symptoms: The router's convergence time is greater than 90 seconds when you clear the multicast routing table.

  Conditions: Occurs with a ring topology with 2 parallel paths from the FHR to the LHR Receivers.

  Workaround: There is no workaround.

- CSCtz90273

  Symptoms: The router duplicates multicast traffic when configured as a static rendezvous point (RP) node.

  Conditions: Occurs under either of the following conditions:

  - You remove Auto RP announce configurations on all routers.
  - You configure the router as a static RP and enable multicast traffic

  Workaround: Select an RP mode: static, auto, or bootstrap router (BSR) and avoid switching dynamically between RP modes.

- CSCtz92857

  Symptoms: MAC learning fails and the router displays FIFO table overflow messages.

  Conditions: Occurs with a MAC security configuration running at high scale.

  Workaround: There is no workaround.

- CSCtz92914

  Symptoms: L3 multicast replication fails on some of the EFPs.

  Conditions: Occurs under the following conditions:

  1. You configure a group of EFPs and map each EVC to a different bridge-domain.
  2. You create a QoS policy-map on each EVC.
  3. All BDI send IGMP joins to single multicast group.
  4. The router initiates multicast data traffic
  5. You remove and reconfigure some of the EFPs

  Workaround: Configure the EFPs and bridge-domains and initiate traffic flow before attaching QoS policies.

- CSCua03439

  Symptoms: The router displays error messages similar to the following:
  %EVENTLIB-3-CPUHOG: SIP0: nile_mgr:

Conditions: Occurs when you boot the router running QoS configurations at a high scale, particularly queues.

Workaround: There is no workaround.

- CSCua12366

  Symptoms: The IOMD process corresponding to OC3 IM (interface module) crashes.

  Conditions: Occurs when you perform an IM OIR after the router has been passing traffic.

  Workaround: There is no workaround; the IM recovers after the crash and resumes traffic.

- CSCua16143

  Symptoms: IPv6 BFD sessions drop after you perform an SSO.

  Conditions: Occurs when you perform an SSO on the router while running an IPv6 BFD configuration. The issue does not occur with an IPv4 BFD configuration.

  Workaround: After SSO, perform a shutdown/no shutdown on the physical interface.

- CSCua16492

  Symptoms: Some IPv6 multi-hop BFD over BGP sessions flap.

  Conditions: Occurs on port-channel interfaces running IPv6 multi-hop BFD over BGP sessions after you perform an SSO.

  Workaround: There is no workaround.

- CSCua25932

  Symptoms: Convergence caused by an interface flap takes more than 50 milliseconds.

  Conditions: Occurs when you enable BGP PIC core and LFA FRR at the same time.

  Workaround: Use LFA FRR, as it converges in less than 50 milliseconds for BGP VPNv4 prefixes.

- CSCua33453

  Symptoms: A CFM configuration crashes after passing traffic for several hours.

  Conditions: Occurs when you create the following configuration:

  - A port-channel interface configured with an EVC and applied to a bridge-domain
  - A physical interface configured as a trunk EFP
  - The **offload sampling** command is configured on both interfaces

  Workaround: There is no workaround.

- CSCua33788

  Symptoms: The router does not pass multicast traffic consistently; only some traffic passes.

  Conditions: Occurs when you configure 255 EVCs spanning across different slots on the router.

  Workaround: There is no workaround.

- CSCua36065

  Symptoms: The router forwards multicast traffic on 63 out of 255 multicast output interfaces (OIFs).

  Conditions: Occurs when you configure the following:

  - 255 EVCs on a single port mapped to 255 BDIs (one EVC per BDI) using rewrite tagging.
  - 255 BDIs which send IGMP v2 Joins to a single multicast group.
  - 255 EVCs configured as a routed port with the port a member link of a port-channel.

  - 255 EVCs configured on a port-channel and sending multicast traffic to a multicast group

  Workaround: There is no workaround.

- CSCua38675

  Symptoms: The router displays a QoS Stats Stalled error message and stops applying QoS configurations.

  Conditions: Occurs when you apply a flat VLAN policy to a trunk EFP interface.

  Workaround: There is no workaround.

- CSCua41400

  Symptoms: QoS classification does not function properly.

  Conditions: Occurs when you create QoS class containing a policy that classifies on both ACL and DSCP value.

  Workaround: There is no workaround.

- CSCua43843

  Symptoms: QoS classification fails when you configure the **match vlan** command under a class-map.

  Conditions: Occurs when the router is configured with an EVC with the **encapsulation default** command.

  Workaround: Change the encapsulation to dot1q.

- CSCua52162

  Symptoms: The router does not learn remote CFM MEPs on EFP interfaces.

  Conditions: Occurs when you configure rewrite push operation on an EFP interface.

  Workaround: There is no workaround.

- CSCua52187

  Symptoms: The router crashes when you attach a QoS policy.

  Conditions: Occurs when you apply a QoS class-map that

  - Matches traffic based on an ACL
  - References an ACL not present in the running configuration
  - Is referenced in a policy with a DSCP marking action

  Workaround: There is no workaround.

- CSCua54547

  Symptoms: The router does not learn remote CFM MEPs.

  Conditions: Occurs under the following conditions:

  - The router is connected to the remote MEPs via a pseudowire connection.
  - The router is configured with MPLS on a bridge-domain interface
  - Dot1q encapsulation is configured on an EFP.

  Workaround: Configure the EFP encapsulation as untagged.

- CSCua55122

  Symptoms: The OC-3 interface module crashes when you create a high number of ATM IMA interfaces.

Conditions: Occurs when you configure multiple ATM IMA interfaces with fewer than 16 links per bundle.

Workaround: Perform a hard OIR on the interface module.

- CSCua56761

  Symptoms: Gigabit Ethernet port 0/5/1 does not timestamp Ethernet OAM Y.1731 packets.

  Conditions: Occurs when you configure Ethernet OAM on port 0/5/1 of a copper or SFP Gigabit Ethernet interface module.

  Workaround: There is no workaround.

- CSCua61909

  Symptoms: Changes to the **police** QoS command do not take effect.

  Conditions: Occurs under the following conditions:

  – You create a QoS policy with a policer and attach the policy to an interface.

  – You make a dynamic change to the police action such as altering the policer value, conform-action value, or exceed-action value.

  Workaround: Remove the policy from the interface, make the necessary changes, and re-attach the policy.

- CSCua67795

  Symptoms: The router does not transmit Y.1731 Delay Measurement Message (DMM) values using QinQ encapsulation.

  Conditions: Occurs with the following configuration:

  – An EFP is configured and applied to a bridge-domain.

  – The EFP is configured with QinQ encapsulation.

  – A Y.1731 Delay Measurement Message (DMM) value is applied.

  – The Y.1731 traffic uses a CoS value other than 0.

  Workaround: There is no workaround.

- CSCua70585

  Symptoms: The router does not update Gigabit Ethernet interface bitmaps after you remove an EFP from a multicast group. The router can display CPU hog messages.

  Conditions: Occurs under the following conditions:

  – You create an EFP on a single bridge-domain interface (BDI)

  – The router receives IGMP v2 or v3 SSM Joins to the BDI

  – You create a second EFP on the same BDI

  – You delete the first or second EFP.

  Workaround: There is no workaround.

- CSCua72298

  Symptoms: The router stops passing traffic on 10-15 HDLC interfaces.

  Conditions: Occurs when you configure a large number of HDLC interfaces: 84 per port or 336 per interface module.

  Workaround: Remove and reconfigure the interface.

- CSCua73104

Symptoms: The router does not increment QoS port shaper policy counters displayed by the **show policy interface** command.

Conditions: Occurs when you configure -A class-default policy on a physical interface -A class-based policy on an EVC interface

Workaround: There is no workaround; however, the router applies the QoS policy normally.

Resolved Caveats—Cisco IOS XE Release 3.7(0)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.7.0S.

- CSCtx00558

  Symptoms: The standby RSP crashes during bootup.

  Conditions: The issue can occur during bootup of a dual RSP system.

  Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCty42336

  Symptoms: BFD sessions flap on the router.

  Conditions: Occurs when the router is running IP BFD sessions in echo mode with 64 200ms X3 timers.

  Workaround: There is no workaround.

- CSCty74129

  Symptoms: A REP topology may reconverge during an RSP switchover. The consoles displays REP no-neighbor messages.

  Conditions: Occurs when you configure REP between two Cisco ASR 903 Routers and you perform an RSP switchover.

  Workaround: There is no workaround.

- CSCty77466

  Symptoms: The port shaper rate changes on RSP switchover.

  Conditions: Occurs under the following conditions:

  - You attach a shaper policy to an interface
  - The interface is configured with multiple EVCs
  - The EVC has a QoS policy attached.

  Workaround: Remove and re-attach the policy on the interface.

- CSCtz03779

  Symptoms: The standby RSP crashes during ISSU.

  Conditions: Occurs when you perform an ISSU downgrade from Release 3.6 to 3.5.

  Workaround: There is no workaround.

- CSCtz09708

  Symptoms: The router cannot establish a PTP session when configured as a PTP slave device.

  Conditions: Occurs when the router receives PTP packets containing a VPN or VRF label.

  Workaround: There is no workaround.

- CSCtz54650

  Symptoms: REP flaps intermittently.

  Conditions: Occurs with a hybrid REP configuration containing ports with and without Fast LSL enabled.

  Workaround: Configure all interfaces with Fast LSL.

- CSCtz56517

  Symptoms: The router drops MPLS packets with a checksum of 0xFFFF.

  Conditions: Occurs when the ASR 903 is acting as a label disposition edge label switch router (LSR).

  Workaround: There is no workaround.

- CSCtz61153

  Symptoms: The ASR 903 does not establish BFD neighbors over port-channel 16.

  Conditions: Occurs when you configure BFD on port-channel 16 between two ASR 903 routers.

  Workaround: Configure BFD on port-channels 1 - 15.

Restrictions and Caveats in Cisco IOS XE 3.8 Releases

This chapter provides information about restrictions and caveats in Cisco IOS XE 3.8 releases.

Note We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

This chapter contains the following sections:

Limitations and Restrictions

The following sections describe the Cisco ASR 903 Router limitations in IO S XE 3.8 releases:

Limitations and Restrictions in Cisco IOS XE Release 3.8(2)S

There are no changes in limitations and restrictions in Cisco IOS XE Release 3.8(2)S; the restrictions from Cisco IOS XE Release 3.8(0)S still apply.

Limitations and Restrictions in Cisco IOS XE Release 3.8(1)S

Cisco IOS XE Release 3.8(1)S introduces the following new limitations:

EFP Limitation

- The Cisco ASR 903 Router supports a maximum of 36 trunk EFPs; this release increases the maximum number from 24 to 36.

All other restrictions from IOS XE Release 3.8(0)S still apply.

Limitations and Restrictions in Cisco IOS XE Release 3.8(0)S

The following limitations apply to the Cisco ASR 903 Router in IOS XE Release 3.8(0)S:

TDM Limitation

- The **configure replace** command is not supported for TDM interfaces.

ATM IMA Limitation

- You can create a maximum of 16 IMA groups on each T1/E1 interface module.
- High Availability (HA) is not supported with IMA.

Bidirectional Forwarding Detection Limitations

- The ASR 903 does not support BFD timers with a value of less than 200 ms x 3 (using a multiplier of 3) for software-based BFD sessions.

Bridge Domain Interface Limitation

- The **mtu** command is not supported on BDI interfaces; however the **ip mtu** command is supported.

Clocking and Timing Limitation

- Only a single clocking input source can be configured within each group of eight ports (0-7 and 8-15) on the T1/E1 interface module using the network-clock input-source command.
- Synchronous Ethernet clock sources are not supported with PTP. Conversely, PTP clock sources are not supported with synchronous Ethernet. However, you can use hybrid clocking to allow the router to obtain frequency using Synchronous Ethernet and phase using PTP.

Dying Gasp Limitations

The ASR 903 supports dying gasp under the following scenarios:

- Ethernet OAM is disabled
- Interface is shut down
- Interface enters error-disabled state
- Router reload

Dying Gasp is not supported in the event of a power failure.

EFP Limitations

- QinQ is not supported on trunk EFP interfaces.
- The Cisco ASR 903 Router supports a maximum of 24 trunk EFPs.

Equal Cost Multipath Limitation

- The Cisco ASR 903 Router supports a maximum of 4 Equal Cost Multipath (ECMP) links.

Ethernet IM Limitations

- The Cisco ASR 903 Router does not support the Facilities Data Link (FDL) on Ethernet interfaces.
- The Cisco ASR 903 Router does not support the **mac-address** command on Gigabit Ethernet interface modules.
- 10 Gigabit Ethernet interface modules are not supported in slots 4 and 5.

- When you install a Gigabit Ethernet IM in the topmost interface module slot (slot 5), the last interface (interface GigabitEthernet0/5/0) is not operational; the port is reserved for internal communication.
- When you configure the copper and SFP Gigabit Ethernet interface modules on a router with redundant RSPs, the **speed** and **duplex** commands are not visible in interface configuration mode until you apply a **shutdown/no shutdown** to the interface.
- Fragmentation is not supported with Multicast traffic.

IPv6 Limitations

The following limitation applies when using IPv6 on the Cisco ASR 903 Router:

- IPv6 Neighbor Discovery (ND) cache timer expiry is 4 hours. To prevent the neighbour adjacency from being deleted after the timer expires:
  - configure hardware based BFD sessions with the neighbours, or
  - configure static IPv6 neighbours, or
  - configure the **ipv6 nd cache expire timer refresh** command.

IS-IS Limitations

- IS-IS over IPv6 is not supported on VRF instances.
- Only one IS-IS process is permitted when you configure IS-IS with the **address-family ipv6** and **bfd-all-interfaces** commands.
- The IS-IS total and per-stream convergence time increases as the number of prefixes increases.

MLPPP Limitations

The following limitations apply when using MLPPP on the Cisco ASR 903 Router:

- All links in an MLPPP bundle must be on the same interface module.
- All links in an MLPPP bundle must be of the same bandwidth.
- The Cisco ASR 903 Router supports a maximum of 8 links per bundle
- To change the MLPPP bundle fragmentation mode between enabled and disabled, perform a **shutdown/no shutdown** on the bundle.
- LFI is not supported
- Multiclass MLP is not supported
- The Cisco ASR 903 Router supports MLPPP statistics with the following limitations:
  - Packet counters on the bundle display the number of fragments rather than packets.
  - Control packets are accounted on the bundle.
- If you increase the maximum transmission unit (MTU) size on an MLPPP interface to a value higher than the maximum received reconstructed unit (MRRU) value on the peer interface, this can bring the MLPPP tunnel down. To restore the tunnel, perform a shutdown/no shutdown on the interface.

MPLS VPN Limitation

- MPLS VPN (L3VPN) Fragmentation does not function properly if an access interface has a higher MTU value than a core interface. To ensure that fragmentation functions correctly, configure the core interface MTU with a value that exceeds the access interface MTU and relevant headers.

OC-3 IM Limitations

- The **configure replace** command is not supported on the OC-3 IMs.
- The optical interface module is designed for OC-3 and OC-12 traffic, but OC-12 functionality is not currently supported.
- MPLS-TP is not supported over POS interfaces.
- Multicast is not supported on POS, MLPPP and OC-12 interfaces.
- MPLS is supported only on PoS and MLPPP interfaces; MPLS on T1/E1 links is not supported.
- IP-FRR and BFD-triggered FRR are not supported on MPLS over POS links.
- Fragmentation is not supported with Multicast traffic on PoS interfaces.
- QoS is not supported with Multicast traffic on PoS interfaces.
- QoS is supported on POS interfaces on optical interface module.
- Three-level QoS policies are not supported on OC-3/OC-12 serial, MLPPP, and PoS interfaces. You can only apply QoS policies on two levels on these interfaces.

Pseudowire/AToM Limitation

- The Cisco ASR 903 Router supports ATM over MPLS N-to-one cell mode for a single ATM Virtual Channel Connections (VCCs) or Permanent Virtual Circuits (PVCs) to a pseudowire, but does not support mapping to multiple VCCs or PVCs.
- The Cisco ASR 903 Router does not support ATM over MPLS one-to-one cell mode.
- The Cisco ASR 903 Router supports pseudowire ping using the CW method; pseudowire ping using the TTL method is not supported.
- The Cisco ASR 903 Router supports a maximum of 2000 pseudowires in any combination.

The following pseudowire (PW) features are supported over MPLS-TP connections:

- ATM over MPLS PWs
- ATM attachment circuits
- AAL5 Encapsulation
- ATM VC Class Support
- Cell Relay including VC mode, VP mode, and Packed Cell Relay
- CESoPSN
- L2VPN pseudowire redundancy
- Multi-segment PWs
- PW OAM/Status TLV Support
- PW Redundancy
- SAToP

The following pseudowire (PW) features are not supported over MPLS-TP connections:

- ATM OAM Cell Emulation for ATM AAL5 over MPLS on PVC and in VC Class.
- BFD / VCCV over ATM AC over MPLS TP
- BFD/ VCCV over TDM PW over MPLS TP Manageability
- Ethernet VLAN to Ethernet VLAN L2VPN interworking (bridged and routed modes)
- Ethernet VLAN to ATM AAL5 L2VPN Interworking (bridged and routed modes)

- Ethernet port to ATM AAL5 PVC L2VPN Interworking (bridged and routed modes)
- Layer 2 QoS features such as classifying or marking based on an L2 value
- MIB support including PW-TDM-MIB, PW-ATM-MIB, and PW-CESOPSN-MIB
- N:1 PVC Mapping with non-unique VPI (N>1)

QoS Limitations

For a description of QoS features and limitations on the Cisco ASR 903 Router in Release 3.8S, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.8.0S/ASR903-Chassis-SW-38.html

Software Upgrade Limitation

- We recommend you set the **interface-module-delay** value to 150 or greater in order to ensure sufficient time for IM software upgrades.

Subinterfaces Limitation

- The Cisco ASR 903 router does not support subinterface configurations except on ATM interfaces.

Note You can configure similar functionality using multiple Ethernet Virtual Connections on an interface. For more information, see Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.

T1/E1 IM Limitations

- Inverting data on the T1/E1 interface is not supported—Inverting the data stream using the invert data interface command is not supported.
- Bit error rate test (BERT) patterns have limited support—Currently, only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported for BERT.
- If you issue the **no card type** command on the controller, you must reload the router in order to configure a new **card type** value.

VPLS BGP Signaling

- TE as core interface is supported for VPLS BGP Signalling but TE as preferred path is *not* supported.
- MAC Flushing is *not* supported in this release for VPLS BGP Signaling.
- Templates are *not* supported in this release for VPLS BGP Signaling.
- Support for H-VPLS is available only for the hierarchical route reflector (RR) model.
- BGP Signaling Inter-AS Option A is supported in this release. BGP Signaling Inter-AS Option B and Inter-AS Option C are *not* supported in this release.
- Maximum number of supported BGP Signaling neighbors per VFI is 32.
- When route designator (RD) is explicitly configured within the same VPLS domain, the virtual forwarding interface (VFI)s with the same VPN ID on different PE's must have the same RD configured (as the auto-generated RD is same for Intra AS). Thus, all the PE's within a VPLS domain must have the same RD. See Example: Configuring VPLS BGP Signaling with Explicit RD Configurations:, page 6.

  For more information, see *VPLS BGP Signaling*.

Example: Configuring VPLS BGP Signaling with Explicit RD Configurations:

```
l2vpn vfi context TEST1
 vpn id 1
autodiscovery bgp signaling bgp
  ve id 1
  ve range 100
  rd 2:1       ---> RD must be same for all the VFI's in all the PE's
  route-target export 2:1
  route-target import 2:1
  no auto-route-target

router bgp 100
bgp graceful-restart
neighbor 209.165.200.224 remote-as 100
neighbor 209.165.200.224 update-source Loopback1
!
address-family l2vpn vpls
  neighbor 209.165.200.224 activate
  neighbor 209.165.200.224 send-community extended
  neighbor 209.165.200.224 suppress-signaling-protocol ldp
exit-address-family
```

Caveats in Cisco IOS XE 3.8S Releases

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in this chapter.

This section describes caveats in Cisco IOS XE 3.8S releases. The following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

The following sections describe the open and resolved caveats in 3.8S Releases:

- Open Caveats—Cisco IOS XE Release 3.8(2)S, page 7
- Resolved Caveats—Cisco IOS XE Release 3.8(2)S, page 12
- Open Caveats—Cisco IOS XE Release 3.8(1)S, page 20
- Resolved Caveats—Cisco IOS XE Release 3.8(1)S, page 23
- Open Caveats—Cisco IOS XE Release 3.8(0)S, page 36

- Resolved Caveats—Cisco IOS XE Release 3.8(0)S, page 43

Open Caveats—Cisco IOS XE Release 3.8(2)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.8(2)S.

- CSCua77688

  Symptom: The router experiences remote CFM MEP flapping.

  Conditions: This issue occurs when the router is connected via a CFM xconnect and the link is running a high traffic rate.

  Workaround: Reduce the rate of traffic.

- CSCub63072

  Symptom: Traffic drop of more than 50ms observed after a network failure occurs even though LFA FRR and BGP PIC Core are configured.

  Conditions: This issue occurs when there is a network failure.

  Workaround: There is no workaround.

- CSCuc08397

  Symptom: When IFM is configured on EVC BD with encapsulation default in the Core, the remote MEPS are not learnt.

  Conditions: This issue occurs when encapsulation default is configured in the Core.

  Workaround: There is no workaround.

- CSCuc59386

  Symptoms: Continuous IOMD crashes occur on OC-3 IM. Interfaces on OC-3 IM are not configurable and the router displays the following error message:

  ```
  "stand-by does not support this command"
  ```

  Conditions: This issue occurs with OC-3 IM in a redundant configuration when an IOMD crash occurs on the active RSP and the standby IOMD session handle is not cleared.

  Workaround: Reload the standby RSP.

- CSCuc62168

  Symptom: FMFP-3-OBJ_DWNLD_TO_CPP_FAILED error messages seen after a HA switchover is performed when the standby RP is booting.

  Conditions: This issue occurs when CFM offloads with a CC interval of 3.3/10/100ms.

  Workaround: There is no workaround.

- CSCuc70509

  Symptom: Packet rate counters (packets per second) are not cleared to 0 when interface goes down.

  Conditions: This issue occurs on all TDM interfaces like serial, MLPPP, and POS. The issue is observed on controller shutdown and not observed on interface shutdown.

  Workaround: There is no workaround.

- CSCuc93653

  Symptom: Replication fails on the newly added BDIs for Trunk EFP.

Conditions: This issue occurs when new BDIs are added to Trunk EFP with static join.

Workaround: Use dynamic join to add the BDIs.

- CSCud04161

  Symptom: The router incorrectly displays a CFM Delay Measurement Message (DMM) value of 0.

  Conditions: This issue occurs under any of the following conditions:

  –You dynamically add a member link to a port-channel.

  –You issue a **shutdown** command followed by **no shutdown** command on a member link of a port-channel.

  Workaround: Wait for PTP to synchronize before configuring DMM scheduling.

- CSCud09142

  Symptom: Fp active errors are displayed after removing the tunnel-tp interface with high-availability configured.

  Conditions: This issue occurs after removing the tunnel-tp interface.

  Workaround: There is no workaround.

- CSCud28982

  Symptom: The router does not process egress QoS marking on an Ethernet service instance.

  Conditions: Occurs when you configure QoS on an Ethernet service instance that is a member of a bridge-domain and uses dot1q encapsulation.

  Workaround: There is no workaround.

- CSCud30554

  Symptom: Object download failure messages are displayed on console during object cleanup. This would cause a possible leak in the hardware resource if the objects are not cleaned up later.

  Conditions: This issue occurs during object cleanup and during the VC deletion.

  Workaround: There is no workaround.

- CSCud37927

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs) and FPGA gets stuck.

  Conditions: This issue occurs under the following conditions:

  – UP MEP and more than one port on the core side connected to the other router.
  – If REP or STP is already configured on core interface, and then UP MEP is configured.
  – REP or STP is running and one of the port is ALT or BLK state and a **shutdown** followed by a **no shutdown** is performed on the interface. Or an OIR of the IM is performed causing REP/STP state changes and the FPGA gets stuck.

  Workaround: There is no workaround.

- CSCud61551

  Symptom: Serial Number of the RSP in slot 1 does not display in the **show inventory** command output.

  Conditions: This issue occurs under unknown conditions.

  Workaround: Reload the router.

- CSCud64436

Symptom: The router does not send the full line rate on POS interfaces.

Conditions: This issue occurs when you send traffic over a POS interface on the OC-3 interface module with a QoS configuration.

Workaround: There is no workaround.

- CSCud89451

  Symptom: The router crashes with an error message showing nmpls_label_populate_flow_data.

  Conditions: This issue occurs when you reset a core interface while the ASR 903 is acting as a PE router and running a configuration with L2VPN and L3VPN.

  Workaround: There is no workaround.

- CSCud98985

  Symptom: Invalid command errors were detected for a few commands.

  Conditions: This issue occurs on executing **show tech-support** command.

  Workaround: There is no workaround.

- CSCud99692

  Symptom: The convergence time takes more than 3 seconds.

  Conditions: This issue occurs in Border Gateway Protocol (BGP) PIC core when path is moved from one active path to 2 Equal Cost Multipath (ECMP) Paths.

  Workaround: There is no workaround.

- CSCue01419

  Symptoms: EIGRP neighborship is lost on OC-3 IM and OC-12 IM interfaces configured on port 0.

  Conditions: This issue occurs on interfaces configured on port 0 of OC-3 IM and OC-12 IM. This issue is not seen on ports 1,2 or 3.

  Workaround: Perform a shutdown followed by no shutdown on interfaces configured on port 0. Alternatively remove EIGRP and configure again.

- CSCue07502

  Symptom: A crash is observed after completing ISSU. The F0/F1 are getting stuck in init state.

  Conditions: This issue occurs after completing ISSU.

  Workaround: Reload the router.

- CSCue16617

  Symptom: The QoS classification does not work in core interfaces.

  Conditions: This issue occurs when the output policy applied to interface has bridge domain interface (BDI) as the core interface.

  Workaround: Enable **mpls ldp explicit null** command.

- CSCue19836

  Symptom: Controller flaps are observed on the CE routers with MR-APS configured on the PE routers with CEM circuit configuration.

  Conditions: This issue occurs when the controllers on CE routers flap. This issue occurs when MR-APS is configured on PEs having CEM circuit for corresponding controllers.

  Workaround: There is no workaround.

- CSCue35103

Symptom: CPU utilization is high after executing the show mac-address-table command.

Conditions: This issue occurs after scaled MAC entries are learned over the BD.

Workaround: Execute the command with reduced term length.

- CSCue40248

  Symptom: Traffic does not flow through newly created MLP interfaces after a switchover is performed.

  Conditions: This issue occurs after you have a newly created MLP interface terminated under a VRF and a switchover is performed.

  Workaround: There is no workaround.

- CSCue43036

  Symptom: %IDBINDEX_SYNC-4-RESERVE traceback seen on OC-12 card type.

  Conditions: This issue occurs after the card type is set the to OC-12 and the router is reloaded. This issue is seen on a HA system with POS configuration.

  Workaround: There is no workaround.

- CSCue51682

  Symptom: The REP protocol flaps, as indicated by the following error messages:

  ```
  *Feb  8 06:51:38.857: %REP-4-LINKSTATUS: GigabitEthernet0/0/1 (segment 10) is
  non-operational due to neighbor not responding
  *Feb  8 06:51:39.096: %REP-4-LINKSTATUS: GigabitEthernet0/0/1 (segment 10) is
  operational
  ```

  Conditions: This issue occurs with REP fast LSL (with lsl-ageout 200msec) is configured and when a burst of new MAC address (usually > 4k) is getting learnt into the system.

  Workaround: Remove fast LSL from the REP configuration

- CSCue54997

  Symptom: Two input clock sources are accepted from same OC-3 IM but the system can support only one input clock source per OC-3 IM.

  Conditions: This issue occurs when two input clock sources are getting accepted from same OC-3 IM.

  Workaround: There is no workaround. Do not configure the second input clock source from same OC-3 IM or remove both OC-3 IM sources and exit the configuration and configure the desired OC-3 IM controller alone.

- CSCue75372

  Symptom: TIME-HOG messages are seen during an IM OIR.

  Condition: This issue occurs when default and IP template is used.

  Workaround: There is no workaround.

- CSCue96886

  Symptoms: Complete MAC Address space is not available on the RSP.

  Conditions: This issue occurs after removing the service instance with the MAC Addresses learnt on the BD.

  Workaround: Reload the Router.

- CSCuf15768

Symptom: Multicast traffic is not bridged with REP.

Conditions: This issue occurs when multicast traffic flows on the REP configured interfaces.

Workaround: Unconfigure and configure REP on the interfaces.

- CSCuf61024

  Symptom: TDM and OC-3 IM continuously crashes enters inserted state after ISSU is performed.

  Conditions: This issue occurs after ISSU is performed.

  Workaround: There is no workaround.

- CSCuf74113

  Symptom: Interface mode cannot be entered for serial interfaces. Error messages are displayed.

  Conditions: This issue occurs after creation of serial interfaces.

  Workaround: There is no workaround.

- CSCuf80482

  Symptom: Configuration synchronization fails from active to standby IOMD.

  Conditions: This issue occurs on IM OIR.

  Workaround: Perform a soft reset of the IM or the interface flap.

- CSCuf86247

  Symptom: SNMP MIB variables related to BDI counters do not function properly.

  Conditions: This issue occurs when you use SNMP MIB variables related to BDI interface counters.

  Workaround: There is no workaround.

- CSCuf89725

  Symptom: After IM OIR the remote MEP shows BLK state on CFM offload.

  Conditions: This issue occurs when CFM MEP is configured an IM OIR is performed.

  Workaround: There is no workaround.

- CSCug05491

  Symptom: The router drops traffic on VPLS circuits.

  Conditions: This issue occurs when the following is performed:

  - Configure REP with or without VLAN load balancing
  - Configure VPLS VFI on the VLANs
  - Issue an stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCug05647

  Symptom: Interface counters do not get updated with IP traffic.

  Conditions: This issue occurs when performing a back-to-back ping on the connected interfaces.

  Workaround: Perform a router reload.

- CSCug39899

  Symptom: Traffic stops flowing through QinQ BDI interface after ARP times out and ARP is removed by shutting the BDI.

Conditions: This issue occurs when static routing is configured, and no routing protocol is configured on the interface.

Workaround: Manually resolve the ARP by pinging the BDI interface.

- CSCug52920

  Symptom: EFP stats does not work after applying the QoS policy on the EFP.

  Conditions: This issue occurs when service policy is applied on the EFP.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.8(2)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.8(2)S.

- CSCub80685

  Symptom: Ping failure observed and BFD or OSPF flaps on BDI shut.

  Conditions: This issue occurs after shutting down the BDI interface which is receiving IPv4 or IPv6 traffic. Similar conditions occur on no EFP or BDI configured or no IP address is configured.

  Workaround: Stop routing traffic into shut BDI port.

- CSCub89304

  Symptom: Remote meps not learnt for CFM UP MEPS on EVC BD.

  Condition: This issue occurs when IP MEPS are configured on EVC BD and Core side has port-channel with Trunk EFP configured.

  Workaround: There is no workaround.

- CSCub89531

  Symptom: Multicast statistics in the MFIB output display NA/NA. This causes multicast traffic to drop every 3 minutes once the 3 minute timer expires.

  Conditions: This issue occurs after an stateful switchover (SSO) is performed.

  Workaround: Issue another SSO or reload the router.

- CSCuc41871

  Symptoms: ATM interfaces stay down during normal operations.

  Conditions: This issue occurs under the following conditions:

  1. Post router reload is performed

  2. Peer interface cable is pulled out & put back in.

  Workaround: Perform an interface reset by issuing the **shutdown** command followed by a **no shutdown** command.

- CSCuc76353

  Symptom: Boot flash is inaccessible in ROMMON and IOS prompt.

  ```
  "dir bootflash:" CLI does't display boot flash contents.
  ```

  Condition: This issue is observed randomly on bootup. This issue is mostly observed when access to the boot flash gets interrupted because of system reload or system crash. In these cases, boot flash goes to unknown state and is not accessible either from the ROMMON or IOS.

  Workaround: Perform an OIR or power cycle of the RSP to recover the boot flash errors.

- CSCud13242

  Symptom: The Cisco ASR 903 router does not display an alarm when nV satellite authentication fails.

  Conditions: This issue occurs when the ASR 9000 and ASR 903 are in an nV satellite configuration and the routers are configured with a different serial-number value.

  Workaround: There is no workaround.

- CSCud26812

  Symptom: The router CLI does not display some SFP PIDs.

  Conditions: This issue occurs when you install one of the following SFPs in the router:

  –ONS-SI-155-L2

  –ONS-SI-155-L1

  –ONS-SI-155-I1

  Workaround: There is no workaround.

- CSCud29479

  Symptom: The router stops applying QoS configurations.

  Conditions: Occurs under the following conditions:

  –An Ethernet interface is configured with a single service instance

  –A QoS policy is attached to the service instance

  –The QoS policy contains a single class containing a match EFP statement.

  –You reset the interface to the default configuration.

  Workaround: There is no workaround.

- CSCud30806

  Symptom: The router accepts a QoS WRED configuration containing **match-all** configurations for two different **prec** values, which is not supported.

  Conditions: This issue occurs when you configure a policy with a class-map containing **match-al**l configurations for two different **prec** values.

  Workaround: There is no workaround.

- CSCud34346

  Symptom: The router crashes with multiple ECMP paths configured.

  Conditions: The issue can occur when:

  –The router is configured with multiple ECMP paths.

  –MPLS IP is not enabled on one of the ECMP paths.

  Workaround: There is no workaround.

- CSCud38038

  Symptom: The router records incorrect delay measurements after a reload.

  Conditions: This issue occurs under the following conditions:

  –You configure Delay Measurement Message (DMM) on a port-channel interface.

  –The port-channel member links are on different interface modules (IMs).

  –You reload the router.

Workaround: You can use the following workarounds:

–Remove the **ethernet cfm global** command and re-apply it after the port-channel member links recover.

–Configure PTP clock synchronization.

- CSCud38589

  Symptom: DMM session stops working.

  Conditions: This issue occurs when DMM is configured on bridge domain UP MEP, with redundant links on the Core side, which are in STP Forwarding or blocked state. The issue is observed when the STP forward port is shut.

  Workaround: Restart the IP SLA session or **unshut** the port and bring it forward state.

- CSCud44942

  Symptom: Remote MEPS are not learnt for port MEPs.

  Conditions: This issue occurs when we configure any EFP on the interface, which has port-me configurations, causing the port MEP to stop working.

  Workaround: There is no workaround.

- CSCud48298

  Symptom: The Cisco ASR 903 dataplane fails on bootup of the CEM PW after a switchover is performed.

  Conditions: This issue occurs after a switchover is performed.

  Workaround: There is no workaround.

  CSCud50944

  Symptom: The router drops traffic on an MLPPP bundle.

  Conditions: This issue occurs following a reload while the router is passing traffic close to the line rate. The issue occurs less frequently with lower traffic rates.

  Workaround: Issue a shutdown/no shutdown on multilink interface.

- CSCud64034

  Symptom: The T1 interfaces do not come up after a SSO.

  Conditions: This issue occurs under the following conditions:

  –Configure T1 interfaces and verify that they come up

  –Perform an SSO

  –Verify the interfaces and check for traffic flowing through the interfaces

  –Unconfigure T1 interfaces.

  –Reload the standby RSP

  –Configure T1 interfaces. The T1 interfaces do not come up.

  Workaround: Perform an IM OIR on the router.

- CSCud76770

  Symptom: Convergence time for FRR link or node protection is more than 2 seconds.

  Conditions: This issue occurs when NNHOP backup tunnels are configured in a ring topology.

  Workaround: There is no workaround.

- CSCud76957

  Symptom: Traffic gets dropped during egress when service instance is configured.

  Conditions: This issue occurs when service instance is configured.

  Workaround: Unconfigure the service instance and reconfigure it again.

- CSCud90890

  Symptom: Routing over Trunk EFP over port-channel does not work on member ports associated with ASIC #1.

  Conditions: This issue occurs when a Trunk EFP on port-channel has members on ASIC#1, the routing traffic does not egress on those ports.

  Workaround: There is no workaround.

- CSCud90955

  Symptom: The following console messages are seen whenever BFD session is created or modified.

```
Jan  3 06:34:52.481: %HANDOFF_FUD-6-QDR_MULTI_BIT_ERROR_START: SIP1: nile_mgr:
Handoff FPGA could encounter MBE,  check at start of create update BFD session
Jan  3 06:34:52.481: %HANDOFF_FUD-6-QDR_MULTI_BIT_ERROR_END: SIP1: nile_mgr:  Handoff
FPGA could encounter MBE, check at end of create update BFD session
Jan  3 06:34:53.167: %HANDOFF_FUD-6-QDR_MULTI_BIT_ERROR_START: SIP0: nile_mgr:
Handoff FPGA could encounter MBE,  check at start of create update BFD session
Jan  3 06:34:53.167: %HANDOFF_FUD-6-QDR_MULTI_BIT_ERROR_END: SIP0: nile_mgr:  Handoff
FPGA could encounter MBE, check at end of create update BFD session
```

  Conditions: This issue occurs when BFD sessions are created or modified.

  Workaround: There is no workaround. This issue has no service impact.

- CSCud96604

  Symptom: On system reset or reload, all traffic on certain Ethernet Flow Point (EFP)s do not egress.

  Conditions: This issue occurs when traffic completely stops on certain EFPs.

  Workaround: Delete and reconfigure EFPs.

- CSCue00049

  Symptom: Classification does not work properly with non-matching traffic when IP ACL is used.

  Conditions: This issue occurs only for class-based ACL match. The ACL class are classified properly and other classes based on DSCP or class-default do not work

  Workaround: There is no workaround.

- CSCue10037

  Symptom: Crash observed on the router.

  Conditions: This issue after when CFM is offloaded and MEPs with 3.3ms were scaled on port-channel with Trunk EFP. This issue occurs after **shutdown** command followed by a **no shutdown** command is executed on the member links of port-channel.

  Workaround: Configure around 50-100 CFM sessions.

- CSCue11444

  Symptom: Split horizon configurations does not clear with Layer2 multicast packets.

  Conditions: This issue occurs when Ethernet Flow Point (EFP)s with split-horizon are configured.

  Workaround: Perform a shutdown followed by no shutdown. Configure EFP first before moving into split-horizon group.

- CSCue16828

  Symptom: Back-to-Back ping failure observed on a PC with Core side Trunk EFP with BDI configured.

  Conditions: This issue occurs when a PC with Core side Trunk EFP with BDI configuration is changed.

  Workaround: Do not change the PC in Core side.

- CSCue18015

  Symptom: S,G does not get created, the forwarding is based on (*,G).

  Conditions: This issue occurs with Interior Gateway Protocol (IGP) change leading to Reverse Path Forwarding (RPF) change of the (*,G).

  Workaround: Clear the (*,G) and recreate it.

- CSCue19898

  Symptom: (*,G) based forwarding is observed with IIF registry change. The Interior Gateway Protocol (IGP) patch change leads to this issue.

  Conditions: This issue occurs when IGP is changed causing a Reverse Path Forwarding (RFP) change notification.

  Workaround: Timeout the (*,G) entry and recreate it again either by issuing **clear ip mroute** command or stopping the joins.

- CSCue20022

  Symptom: Software forwarding of core encapsulation entries causes interface to flap.

  Conditions: This issue occurs when interface has Protocol Independent Multicast (PIM) enabled on the BDI interface.

  Workaround: Perform a soft interface module OIR. Clear the multicast routes for that VRF.

- CSCue25146

  Symptom: The standby OC-3 IM gets reloaded after the controller flaps in active console.

  Conditions: This issue occurs after configuring ATM and Controller and a **shutdown** command followed by a **no shutdown** command is issued when the controller in active.

  Workaround: There is no workaround.

- CSCue25267

  Symptom: The standby RSP reloads on an OC-3 interface module OIR on the active RSP. A crash was observed but core file generated is incomplete.

  Conditions: This issue occurs when the active RSP is booted up first followed by the standby RSP. This issue occurs when APS configurations with serial links are present on the router and IM OIR is performed.

  Workaround: There is no workaround.

- CSCue25567

  Symptom: Quack authentication failure message seen on console.

  Conditions: This issue is seen randomly.

  Workaround: Reload the router.

- CSCue27652

  Symptom: ATM interfaces get deleted after SSO is performed.

  Conditions: This issue occurs after an the ATM interfaces are deleted on the standby RSP after an IM OIR is performed.

  Workaround: There is no workaround.

- CSCue30481

  Symptom: The router does not lock to the syncE clock source after reload. It will be in Ql-failed state.

  Condition: Reload the router with saved syncE configuration.

  Workaround: Unconfigure and configure the clock source.

- CSCue32753

  Symptom: The OC-3 interface modules are lost after a In Service Software Upgrade (ISSU) is performed on the Cisco ASR 903 router and configuration mismatch errors are displayed on router console. The standby RSP reaches standby-hot state causing continuous IOMD crash messages at regular intervals.

  Conditions: This issue occurs when ISSU is performed.

  Workaround: There is no workaround.

- CSCue34597

  Symptom: CHAP authentication process timed out. The PPP interface and multilink bundle does not come up.

  Conditions: This issue occurs when PPP or MLPPP is configured and PPP authentication is enabled.

  Workaround: Remove CHAP authentication from interface.

- CSCue40020

  Symptom: Interior Gateway Protocol (IGP) flap or MPLS-enabled interface flap with 600 Layer2 VPN configured and 6000 Layer3 VPN configured can cause a crash.

  Conditions: This issue occurs after the IGP flaps continuously.

  Workaround: Configure IGP routes less than 100. Scale of Layer2 or Layer3 VPN configuration should be less than 100 to avoid a crash.

- CSCue42315

  Symptom: CPU hog messages and IOMD crash observed on the Cisco ASR 903 router.

  Conditions: This issue occurs with OC-3 interface module after executing the shutdown command followed by a no shutdown command of the multilink bundle when traffic is sent with a packet size greater then 1500 byte.

  Workaround: There is no workaround.

- CSCue43250

  Symptom: IMA configurations cannot be parsed correctly after a router reload.

  Conditions: This issue occurs after the A903-IM40S is inserted in bay 4 or bay 5 of the Cisco ASR903 router and when the IMA and ATM interfaces are adjacent.

  Workaround: Insert the IM in bay 0 or bay 3 for the IMA and ATM parsing to work or reconfigure the ATM and IMA interfaces.

- CSCue45306

  Symptoms: CEM circuits configured over TDM IM go down after SSO is performed.

  Conditions: This issue occurs after a SSO is performed.

  Workaround: Perform a router reload.

- CSCue47317

  Symptom: ISSU may get impacted due to synchronization damage.

  Conditions: This issue occurs after modifying the TDL structures.

  Workaround: There is no workaround.

- CSCue50128

  Symptom: FMFP download failure occurs on reaching 1980 odd number even though 2000 ternary content addressable memory (TCAM) space is allocated for ACLs in the IP template.

  Conditions: This issue occurs in normal conditions when the scale reaches 1980.

  Workaround: There is no workaround.

- CSCue52298

  Symptom: TI/EI interfaces on interface module are lost as IOMD crashes after a switchover.

  Conditions: This issue occurs after IOMD crashes when a switchover was performed.

  Workaround: There is no workaround.

- CSCue52774

  Symptom: Sonet controller as input clock source does not get selected on A900-IMA4OS interface module on a Cisco ASR 903 router.

  Condition: This issue occurs when the port above 0 is used for the clock source.

  Workaround: Use port 0 for clock source or insert the SFP in the odd port (protect port) adjacent to the actual port using an optical splitter. The cable is fed to the odd port to recover the proper clocking for the port.

- CSCue52968

  Symptom: Ping failure occurs and traffic stops through Multilink bundle when Challenge Handshake Authentication Protocol (CHAP) authentication is enabled.

  Conditions: This issue is seen when Policy Feature Card (PFC) and Control Field Compression (ACFC) is configured on the Cisco ASR 903 router.

  Workaround: There is no workaround.

- CSCue57670

  Symptom: The active RSP synchronization LED displays the state incorrectly.

  Condition: This issue occurs after a Stateful Switchover (SSO) is performed without any network clock configuration.

  Workaround: There is no workaround. This issue is a cosmetic issue.

- CSCue59544

  Symptom: The A900-IMA16D generates a storm on closing the backup tunnel.

  Condition: This issue occur after closing the tunnel.

  Workaround: There is no workaround.

- CSCue66137

  Symptom: The IOMD crashes with CPU hog messages.

  Conditions: This issue occurs with OC-3 interface module and traffic is sent over a multilink bundle with packet size greater than 600 byte.

  Workaround: There is no workaround.

- CSCue77612

  Symptom: MAC address synchronization on 1 Gigabit Ethernet port on standby RSP causes traffic to be forwarded to incorrect port after a switchover.

  Conditions: This issue occurs after a switchover.

  Workaround: Clear MAC address after a switchover is performed.

- CSCue86696

  Symptom: Interface flaps are observed after longevity run is performed.

  Conditions: This issue occurs after prolonged tests are performed with SPF interface modules.

  Workaround: There is no workaround.

- CSCue87542

  Symptom: Deleting bridge domain interfaces (BDIs) with routing traffic causes a flood to CPU resulting in control plane traffic loss.

  Conditions: This issue occurs after a ping failure and the Bidirectional Forwarding Detection (BFD) protocol or OSFP protocol flaps on deleting the BDI while IPv4 traffic is flowing.

  Workaround: Delete the Trunk EFP interface and then the BDI.

- CSCue89503

  Symptom: The power supply status displays critical after removing and inserting the power supply on the Cisco ASR903 router.

  Conditions: This issue occurs after multiple OIR of the power supply is performed.

  Workaround: There is no workaround. This issue is cosmetic.

- CSCuf05039

  Symptom: I2C-WRITE and MDIO_READ error messages are displayed on the Cisco ASR903 router.

  Conditions: This issue occurs after an interface module hard or soft OIR is performed.

  Workaround: There is no workaround.

- CSCuf61365

  Symptom: Virtual circuit counters do not increment after interface module Online Insertion and Removal (OIR) followed by a SSO is performed.

  Conditions: This issue occurs after an OIR followed by a SSO is performed.

  Workaround: Perform a SSO without a interface module OIR.

- CSCuf65040

  Symptom: 1 Gigabit Ethernet or 10 Gigabit Ethernet interface module enters out of service state.

  Conditions: This issue occurs when a hard Online Insertion and Removal (OIR) is performed on the interface module.

  Workaround: Perform another hard OIR or a Stateful Switchover (SSO) followed by a soft OIR.

- CSCuf79504

  Symptom: ATM Virtual Channel Connections (VCCs) creation on standby RSP fails.

  Conditions: This issue occurs after issuing **shutdown** command followed by **no shutdown** command on the multiple controller on active RSP.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.8(1)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.8(1)S.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

  Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCtz65778

  Symptom: The control plane goes down with VPNv6 traffic.

  Conditions: Occurs with 64-byte VPNv6 traffic. The issue only occurs for small, tunnelled packets.

  Workaround: There is no workaround.

- CSCua57325

  Symptom: The router displays an OIR SPA error.

  Conditions: Occurs under the following conditions:

  - The router is running offloaded CFM sessions over an xconnect (pseudowire) interface.
  - The router is using a redundant hardware (dual RSP) configuration.
  - The remote router is using a non-redundant (single RSP) hardware configuration.
  - You reload the router.

  Workaround: There is no workaround.

- CSCua77688

  Symptom: The router experiences remote CFM MEP flapping.

  Conditions: Occurs when the router is connected via a CFM xconnect and the link is running a high traffic rate.

  Workaround: Reduce the rate of traffic.

- CSCub18160

  Symptom: The router drops traffic on a link twice and displays a remote fault error message.

  Conditions: Occurs when you issue an interface module reset (OIR) while the 10.000M XFP (DWDM Edge performance) or XFP10GER-192IR-L XFPs are plugged into the ten Gigabit Ethernet interface module and active.

  Reloading the router also takes significantly longer when using these XFPs.

Workaround: There is no workaround.

- CSCub41772

  Symptom: Router console is flooded with CPUHOG and EVENTLIB messages.

  Conditions: The issue occurs rarely when you issue multiple interface module reset (OIRs), RSP switchovers (SSO), or reloads while using a configuration with a high number of T1 serial links on the OC-3 interface module.

  Workaround: There is no workaround; however, the messages to not affect router functionality.

- CSCuc66393

  Symptom: The router loses OC-3 interface configurations after an ISSU upgrade.

  Conditions: Occurs on OC-3 serial and POS interfaces after an ISSU software upgrade.

  Workaround: There is no workaround.

- CSCud01908

  Symptom: The **show platform software object-manager fp active statistics** command shows pending objects on the Forwarding Manager (FMAN) on the forwarding processor (FP), indicating a failure to download configurations from the Route Switch Processor (RSP) to the data plane (DP).

  Conditions: Occurs when you apply a QoS shaping configuration at a high scale.

  Workaround: There is no workaround.

- CSCud06772

  Symptom: IPv6 neighbor discovery does not function properly after stateful switchover (SSO); the router loses traffic and eventually recovers.

  Conditions: Occurs with IPv6 traffic after stateful switchover (SSO).

  Workaround: Configure software BFD sessions.

- CSCud07085

  Symptom: The serial interface on the OC-3 interface module remains in a down state.

  Conditions: Occurs when you migrate from T1 mode to E1 mode using the OC-3 interface module.

  Workaround: Issue an interface module reset (OIR) on the OC-3 interface module.

- CSCud23647

  Symptom: BDI adjacency fails on the standby RSP.

  Conditions: The issue can occur during an interface module (IM) reset or router reload.

  Workaround: There is no workaround.

- CSCud27333

  Symptom: The router crashes continuously.

  Conditions: Occurs when you issue an interface module reset (OIR) while the standby RSP is booting.

  Workaround: Do not issue an interface module reset (OIR) while the standby RSP is booting.

- CSCud29479

  Symptom: The router stops applying QoS configurations.

  Conditions: Occurs under the following conditions:

  – An Ethernet interface is configured with a single service instance

  - A QoS policy is attached to the service instance
  - The QoS policy contains a single class containing a **match efp** statement.
  - You reset the interface to the default configuration.

  Workaround: There is no workaround.

- CSCud33906

  Symptom: Equal Cost Multipath (ECMP) loopback does not function properly.

  Conditions: Occurs when a port-channel link dynamically assigned as an ECMP path.

  Workaround: There is no workaround.

- CSCud56262

  Symptom: The router stops passing traffic on virtual circuits.

  Conditions: Occurs an MPLS-TE/FRR configuration with L2VPN after you issue a stateful switchover (SSO).

  Workaround: Reload the router.

- CSCud64436

  Symptom: The router does not send the full line rate on POS interfaces.

  Conditions: Occurs when you send traffic over a POS interface on the OC-3 interface module with a QoS configuration.

  Workaround: There is no workaround.

- CSCud89451

  Symptom: The router crashes with an error message showing nmpls_label_populate_flow_data.

  Conditions: Occurs when you reset a core interface while the ASR 903 is acting as a PE router and running a configuration with L2VPN and L3VPN.

  Workaround: There is no workaround.

- CSCud95359

  Symptom: The show policy map command displays an incorrect number of total dropped packets (total drops).

  Conditions: Occurs when you issue the show policy-map command to display dropped packets on an interface.

  Workaround: There is no workaround.

- CSCue01419

  Symptom: The router loses EIGRP neighborship.

  Conditions: Occurs on OC-3 and OC-12 interface configured on port 0.

  Workaround: Issue a **shutdown/no shutdown** on interfaces configured on port 0. You can also remove and reconfigure EIGRP.

- CSCue43205

  Symptom: The router drops traffic when you set an interface to the default configuration.

  Conditions: Occurs when you set an interface with QoS configurations to the default configuration. The issue occurs most often with the Ten Gigabit Ethernet interface using a full global configuration.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.8(1)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.8(1)S.

- CSCty30951

  Symptom: The router displays the following console error message: %QOSMGR-3-OUT_OF_TCAM_RESOURCES: SIP0: nile_mgr: Out of tcam resources to execute command

  Conditions: Occurs when you remove a QoS configuration by setting the interface to the default configuration.

  Workaround: There is no workaround.

- CSCty70119

  Symptoms: Port shaper rate changes do not take effect.

  Conditions: Occurs when QoS policies attached to EVCs on an interface do not include a shaper configuration; the issue does not occur on EFP policies that include a shaper in a class.

  Workaround: Include a shaper in one class of the EFP policy.

- CSCtz03919

  Symptoms: The router fails to store trace logs.

  Conditions: Occurs when the /bootflash directory is full.

  Workaround: Clean up the /bootflash and then reboot the router.

- CSCtz20839

  Symptoms: IMA functionality does not work properly.

  Conditions: Occurs after an RSP switchover when the router is running an IMA configuration.

  Workaround: Reload the interface module with the IMA configuration.

- CSCua62029

  Symptom: The router crashes.

  Conditions: Occurs when you configure a class-based QoS policy with the following characteristics:

  - The policy is attached to the main interface.
  - The policy classifies on multiple VLANs.
  - The classification statements specify a priority.
  - The classification statements are within a child QoS policy.

  Workaround: There is no workaround.

- CSCua73104

  Symptoms: The router does not increment QoS port shaper policy counters displayed by the **show policy interface** command.

  Conditions: Occurs when you configure

  - A class-default policy on a physical interface
  - A class-based policy on an EVC interface

  Workaround: There is no workaround; however, the router applies the QoS policy normally.

- CSCua95873

  Symptoms: The router continues passing traffic on the OC-3 interface after you shut down the controller.

  Conditions: Occurs when you shut down the OC-3 controller; the router momentarily continues to increment interface counters.

  Workaround: There is no workaround.

- CSCub73405

  Symptom: Cisco ASR903 router can experience latency for process-switched traffic and display high CPU utilization at nile_mgr.

  Conditions: Occurs on an ASR 903 with redundant RSPs after you reload the standby RSP.

  Workaround: Reboot the router.

- CSCub78861

  Symptom: Following a reload, the router handles CFM only on 128 VLANs or bridge-domains.

  Conditions: Occurs when the router configuration contains CFM and more than 128 VLANs or bridge-domains.

  Workaround: There is no workaround.

- CSCub79869

  Symptom: BGP PIC edge convergence time is high.

  Conditions: Occurs in a 3-label stack setup using LDP, BGP, and VPN labels.

  Workaround: There is no workaround for a stack using 3 labels. However, the issue does not occur when you use 2 labels.

- CSCub98691

  Symptom: The router displays an I2C write fail error message.

  Conditions: The issue can occur when the router is idle or when the router is loaded and passing traffic.

  Workaround: There is no workaround. However, the issue does not have any functional impact.

- CSCuc01154

  Symptom: The router does not report B1, B2, and B3 alarms at normal thresholds.

  Conditions: Occurs on the OC-3 interface module when the router sends errored frames.

  Workaround: There is no workaround.

- CSCuc41763

  Symptom: The router displays a RUNHOG traceback error message.

  Conditions: Occurs when you reload the router or an interface module.

  Workaround: There is no workaround.

- CSCuc51051

  Symptom: Remote LFA FRR convergence takes more than 50 milliseconds.

  Conditions: Occurs after you reload the router.

  Workaround: Reset the interface on the primary path.

- CSCuc58371

  Symptom: Some links do not become active on the OC-3 interface module.

  Conditions: Occurs on the OC-3 interface module (IM) configured at a high scale after you perform a multiple soft OIRs on the IM. The issue occurs frequently with SONET framing.

  Workaround: You can use the following workarounds:

  - Apply a **shutdown/no shutdown** to the OC-3 controller.
  - Re-apply the PDH configuration.
  - Add and remove a loopback configuration on the PDH.

  Add and remove a loopback configuration on the OC-3 controller.

- CSCuc64654

  Symptom: The router is unable to ping the remote customer edge (CE) router.

  Conditions: Occurs when the router is acting as a provider edge (PE) device and is connected to the remote PE using dual loopback interfaces for peering with iBGP sessions.

  Workaround: Use a single loopback interface. Use the same loopback interface for IPv4 and VPNv4 address families.

- CSCuc66393

  Symptom: The router loses OC-3 interface configurations after an ISSU upgrade.

  Conditions: Occurs on OC-3 serial and POS interfaces after an ISSU software upgrade.

  Workaround: There is no workaround.

- CSCuc68462

  Symptom: The router drops PTP traffic.

  Conditions: The issue occurs occasionally when you configure PTP slave clock to receive VLAN-tagged traffic.

  Workaround: There is no workaround.

- CSCuc71723

  Symptom: The router erroneously accepts a service-policy configuration on a CEM interface and displays it within the running configuration.

  Conditions: Occurs when you configure a service-policy on a CEM interface.

  Workaround: There is no workaround.

- CSCuc85721

  Symptom: The router crashes.

  Conditions: Occurs under the following conditions:

  - MR-APS is configured on serial interfaces on the OC-3 interface module
  - The router is configured with a high number of serial interfaces
  - You reset an interface module or reload the router.

  Workaround: There is no workaround.

- CSCuc90008

  Symptom: The OC-3 controller stops passing traffic.

  Conditions: Occurs after you reset the facing interface on the CE device.

Workaround: Reset the interface module.

- CSCuc91007

  Symptom: A slave clock displays a high 1PPS offset value from the master clock.

  Conditions: Occurs after an interface module reset or stateful switchover (SSO) on the master device.

  Workaround: There is no workaround.

- CSCuc92953

  Symptom: The RSP crashes.

  Conditions: Occurs under the following conditions:

  – You configure Protocol-Independent Multicast-Sparse Mode (PIM-SM) with a static rendezvous point (RP).

  – You create an EVC port channel on the access side with one member link

  – You create bridge domain interfaces (BDIs) with 1:1 mapping between EVCs and bridge-domains.

  – You use the BDIs to send IGMP v2 static join messages to a single multicast group

  – On the remote device, you create 150 EFPs and map them to the BDIs.

  – You initiate multicast traffic.

  – You set the EFPs to the default configuration and add them to the existing port-channel

  The router crashes.

  Workaround: There is no workaround.

- CSCuc95590

  Symptom: The router does not automatically upgrade the FPGA software.

  Conditions: Occurs when you load a new image while running an older FPGA version.

  Workaround: There is no workaround; however the issue has no functional impact.

- CSCuc95716

  Symptom: FPGA software for the OC-3 interface module is not bundled with the XE 3.8 image.

  Conditions: Occurs when upgrading FPGA on the OC-3 interface module.

  Workaround: Manually upgrade the OC-3 FPGA.

- CSCuc98185

  Symptom: One out of 48 EFPs in a BDI does not receive traffic when running L3 multicast. The issue does not happen consistently.

  Conditions: Occurs under the following conditions:

  – You configure Protocol-Independent Multicast-Sparse Mode (PIM-SM) with a static rendezvous point (RP).

  – You configure a bridge domain interface (BDI) on the PE2 access side

  – You use the BDI to send IGMP v2 static join messages to a single multicast group

  – You disable IGMP snooping globally.

  – You configure 24 EFPs and map them to a single bridge-domain.

  – You initiate multicast traffic.

  - With multicast traffic enabled, you configure 24 EFPs and map them to the existing bridge-domain.

  One of the 48 EFPs does not receive traffic.

  Workaround: Reload the router.

- CSCud01641

  Symptom: The standby RSP resets when you issue the write memory command on the active RSP.

  Conditions: Occurs under the following conditions:

  - The BITS interface is configured as an input clock source.
  - Quality level-based clock selection is enabled.

  Workaround: Disable QL-enabled mode for network-clock synchronization.

- CSCud01644

  Symptom: The active forwarding processor (FP) is on the standby route switch processor (RSP).

  Conditions: Occurs when you boot the two RSPs in quick succession and the FP on the standby RSP becomes active before the FP on the active RSP.

  Workaround: Reload the router.

- CSCud06744

  Symptom: The router does not download MPLS global prefixes.

  Conditions: Occurs under the following conditions:

  - You configure Loop Free Alternate Fast Reroute (LFA FRR) at a high scale.
  - The primary or backup paths flap multiple times.

  Workaround: There is no workaround.

- CSCud07642

  Symptom: The ASR 903 is unable to pass traffic to the ASR 9000.

  Conditions: Occurs with a clear-channel ATM over MPLS configuration using AAL0 encapsulation.

  Workaround: Enable MPLS control-word on the ASR 9000.

- CSCud07854

  Symptom: FPGA software upgrade fails.

  Conditions: Occurs when you upgrade the FPGA software using an IOS image bundled with a new FPGA version.

  Workaround: Manually upgrade the FPGA software.

- CSCud08913

  Symptom: The router crashes.

  Conditions: The issue occurs in rare instances when you perform an interface module (IM) reset (OIR) on the OC-3 interface module.

  Workaround: There is no workaround.

- CSCud09246

  Symptom: The router crashes.

  Conditions: Occurs under the following conditions:

  - You issue the **clear ip route *** command
  - You issue an interface module reset (IM OIR)

  Workaround: There is no workaround.

- CSCud09315

  Symptom: The show ptp clock running domain 0 and show platform ptp all commands do not display a configured slave clock.

  Conditions: Occurs when you issue a **shutdown/no shutdown** on the link between a boundary clock and a master clock during while the boundary clock is in phase alignment.

  Workaround: Remove and restore the PTP configuration on the boundary clock.

- CSCud12587

  Symptom: When handling IS-IS packets, the router punts the traffic to the Route Switch Processor (RSP) and applies policing to limit the traffic to 1 Mbps.

  Conditions: Occurs when you enable IS-IS over an Ethernet over MPLS (EoMPLS) connection.

  Workaround: Use IS-IS over another connection type or limit the IS-IS traffic to less than 1 Mbps.

- CSCud13535

  Symptom: The router drops imposition traffic sent to a neighbor device over a VPLS pseudowire.

  Conditions: Occurs when the neighbor device configuration includes the **no split horizon group** command.

  Workaround: Remove the **no split horizon group** command from the VPLS neighbor device.

- CSCud15740

  Symptom: The Gigabit Ethernet interface module crashes.

  Conditions: Occurs when the router receives a flood of Wintegra interrupt packets.

  Workaround: There is no workaround.

- CSCud15785

  Symptom: The router experiences flapping on REP connections.

  Conditions: Occurs under the following conditions:

  - MAC limiting is enabled and a MAC address is at the maximum value
  - REP is configured with a 200 millisecond LSL ageout timer

  Workaround: Increase the REP timer to above 500 milliseconds or disable the MAC limiting feature.

- CSCud15841

  Symptom: The clear ip mroute * command can cause resource leakage.

  Conditions: Occurs when you issue the clear ip mroute * command while IP multicast is enabled.

  Workaround: Reload the router.

- CSCud17457

  Symptom: The router drops IP multicast traffic.

  Conditions: Occurs when you perform the following actions:

  - Configure EFPs as members of a port channel containing a single interface.
  - Remove the configuration for the EFPs

  - Remove the interface from the port channel
  - Add the EFPs back onto the interface

  Workaround: Reload the router or issue a stateful switchover (SSO).

- CSCud19563

  Symptom: The T1/E1 interface module on the standby RSP crashes repeatedly.

  Conditions: Occurs when the standby RSP is booting and there is a clock configured on the T1/E1 controller.

  Workaround: Remove the clock configuration prior to booting the standby RSP and restore the configuration afterwards.

- CSCud22601

  Symptom: MPLS-TP tunnels remain down after the standby RSP boots.

  Conditions: Occurs when you boot the standby RSP after applying an MPLS-TP configuration and performing an SSO. The issue occurs rarely.

  Workaround: Issue a shutdown/no shutdown on the MPLS-TP tunnel. A nonintrusive workaround is to cause a flap on the protect label switched path (LSP) by reconfiguring the path or physically shutting down and restoring the interface.

- CSCud23698

  Symptom: The router stops applying classification and marking for a class.

  Conditions: Occurs when you remove a priority level while using dual priority for the

  class-map.

  Workaround: Remove and reattach the policy-map on the interface.

- CSCud24704

  Symptom: The router crashes.

  Conditions: Occurs when you perform an interface module OIR (reset) on the gigabit Ethernet interface module while the standby RSP is booting.

  Workaround: Perform the IM OIR after the standby RSP boots.

- CSCud25813

  Symptom: The router drops IP Multicast traffic.

  Conditions: Occurs under the following conditions:

  - You initiate multicast traffic to a single L3M group.
  - You configure 50 EFPs with corresponding bridge domain interfaces (BDIs) and initiate IGMPv2 join traffic to a single multicast group.
  - You add 25 EFPs with 25 bridge-domain interfaces (BDIs) at a 1:1 ratio.
  - You remove 10 EFPs from the group of 50 and add the same EFPs to the group of 25.
  - The newly added EFPs do not receive any traffic.

  Workaround: Reload the router or issue a stateful switchover (SSO).

- CSCud26154

  Symptom: The router displays incorrect ENV readings.

  Conditions: Occurs when you switch off one power supply unit in a dual power supply configuration.

Workaround: There is no workaround. However, the issue does not have any functionality impact on the system.

- CSCud26240

  Symptom: The router displays Nile mgrs leak error messages.

  Conditions: Occurs when you configure L3VPN and L2VPN services at a high scale.

  Workaround: There is no workaround.

- CSCud26382

  Symptom: The router drops traffic on an EFP interface after you perform a stateful switchover (SSO).

  Conditions: Occurs under the following conditions:

  - You boot the standby RSP
  - The router configuration contains an EFP interface on a Gigabit Ethernet port and a bridge domain interface in a down state.
  - After the router reaches an SSO state, you issue a no shutdown command on the peer router to bring the EFP interface up.
  - You perform an stateful switchover (SSO) on the router.

  Workaround: Issue a shutdown/no shutdown on the gigabit Ethernet port.

- CSCud28553

  Symptom: The router stops passing Switch Port Analyzer (SPAN) traffic.

  Conditions: Occurs after you apply a **shutdown/no shutdown** on the SPAN source port with Ethernet flow point (EFP) and bridge domain interface (BDI) configurations.

  Workaround: Enable and disable the SPAN session

- CSCud28685

  Symptom: Ping fails between the CE1 and CE2 devices when the ASR 903 is acting as the PE device.

  Conditions: Occurs when the SONET controller or ATM interface experiences an interface flap.

  Workaround: Perform a soft OIR on the interface module.

- CSCud28787

  Symptom: The 10 gigabit Ethernet interface module (IM- A900-IMA1X) flaps.

  Conditions: Occurs when the IM passes high traffic volumes for an extended period of time.

  Workaround: There is no workaround.

- CSCud31852

  Symptom: The router displays traffic polarization with L3VPN traffic.

  Conditions: Occurs under the following conditions:

  - The P router has multiple ECMP paths
  - The ECMP paths are port-channels

  Traffic is distributed between ECMP paths, but polarization occurs on the port-channel member links.

  Workaround: There is no workaround.

- CSCud33298

  Symptom: The router crashes.

  Conditions: Occurs when the peer device shuts down.

  Workaround: There is no workaround.

- CSCud33822

  Symptom: The router drops VPN traffic on an MPLS-TE tunnel using an explicit-null label advertisement after tunnel recovery.

  Conditions: The issue occurs under specific network conditions where TE is LDP-enabled and runs over a 10G link with dampening enabled. VPN prefixes are advertised from route-reflector as well as from the VPN PE over the TE tunnel. The TE tunnel is delayed and this causes label forwarding to switch from the 2 stack labeled path to the 3 stack labeled path with same VPN label coming from 2 sources.

  Workaround: Issue a **shutdown/no shutdown** on the tunnel or protect the tunnel from going down using fast reroute (FRR).

- CSCud36431

  Symptom: Backup path is not programmed properly for global prefixes and can cause the cut-over to have a higher convergence time.

  Conditions: Occurs when the router is running remote LFA FRR in a ring with 7 or more routers and one of the router in the ring reloads.

  Workaround: Issue a **shutdown/no shutdown** on the backup or primary interface.

- CSCud38115

  Symptom: OSPF connections flap and drop traffic for approximately 20 seconds

  Conditions: Occurs during stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCud38123

  Symptom: The router drops traffic and displays error messages similar to the following: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: SIP1: fman_fp_image: LENTRY 0xXXXXXXXXX (InLabel XX Table 0) download to CPP failed

  Conditions: Occurs when the primary path flaps more than 15 times while the router is configured with 8000 global prefixes

  Workaround: Reload the router.

- CSCud38164

  Symptom: The router displays an Object download failure message on the console.

  Conditions: Occurs when the number of ip routes reaches its maximum configurable limit.

  Workaround: There is no workaround.

- CSCud38433

  Symptom: The router is unable to establish MPLS neighborship or ping the destination loopback interface.

  Conditions: Occurs when you configure two Equal Cost Multipath (ECMP) paths on a bridge domain interface (BDI) using static routes.

  Workaround: The following workarounds exist:

  - Use Interior Gateway Protocol (IGP) instead of static IP routes.
  - Shut down one of the ECMP paths.

- CSCud38592

  Symptom: The router displays an fman_fp crash error and crashes.

  Conditions: Occurs when the router is running Remote LFA with a high number of prefixes and there is an interface flap on the primary path.

  Workaround: There is no workaround.

- CSCud38668

  Symptom: The OC-3 interface module crashes.

  Conditions: Occurs when you issue the **show platform software agent iomd 1/0 driver peek** command.

  Workaround: There is no workaround.

- CSCud40930

  Symptom: Some interfaces within a bridge-domain are unable to send outbound L3 multicast traffic.

  Conditions: Occurs when the bridge-domain contains EFP interfaces, some of which are on a port-channel. The issue can also occur after a router reload.

  Workaround: Issue a **shutdown/no shutdown** on the BDI interface.

- CSCud42315

  Symptom: The OC-3 interface module crashes.

  Conditions: Occurs when you apply the **forward-alarm ais** command on a T1 controller.

  Workaround: There is no workaround.

- CSCud43580

  Symptom: The router does not apply the **bandwidth remaining percent** command within a QoS policy in some instances.

  Conditions: The issue can occur occasionally when:

  - There is a large discrepancy in **bandwidth remaining** values between QoS classes
  - The classes containing the **bandwidth remaining** statements are oversubscribed at a low rate or have a low queue-limit.

  Workaround: Apply the following workaround:

  - Increase the **queue-limit** value to 120 kilobytes or above.
  - If the QoS configuration uses WRED, increase the minimum threshold value.
  - Alter the bandwidth remaining values to reduce the ratio between values.

- CSCud44640

  Symptom: The router displays a traceback error when there one power supply unit slot is empty.

  Conditions: Occurs during boot.

  Workaround: There is no workaround.

- CSCud44768

  Symptom: Multilink bundles and member links flap when passing traffic.

Conditions: Occurs under the following conditions:

- You configure more than 210 MLPPP bundles with one member link per bundle or 16 bundles with 16 member links each.
- The line is operating at a 64 or 128 byte line rate

Workaround: There is no workaround.

- CSCud49684

  Symptom: The router displays an FMAN-FP memory leak error message.

  Conditions: Occurs when you configure L3VPN at a high scale.

  Workaround: There is no workaround.

- CSCud49980

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs when you configure CFM MEPs on carrier edge (CE) routers and VPLS on provider edge (PE) routers.

  Workaround: Create an EVC bridge-domain running CFM on the PE router and enable a virtual forwarding interface (VFI) on the bridge-domain.

- CSCud50851

  Symptom: The router experiences flapping on REP connections.

  Conditions: Occurs when you enable MAC limiting at a high scale and the set of MAC addresses changes continuously.

  Workaround: Disable MAC limiting.

- CSCud54092

  Symptom: The router displays an error message indicating a crash at tdl_netsync_clk_src_message_create.

  Conditions: The issue can occur when the router is shutting down during a reload

  Workaround: There is no workaround.

- CSCud55377

  Symptom: The router crashes.

  Conditions: Occurs when you configure offloaded CFM for xconnect sessions at a high scale.

  Workaround: There is no workaround.

- CSCud55695

  Symptom: When you apply an QoS policy with a port level class-default configuration containing a shaper value to a serial interface. the router applies the shaper value to the channel-level PIR for all serial interfaces on the IM.

  Conditions: Occurs when you apply QoS policy with a port level class-default configuration containing a shaper value to a serial interface.

  Workaround: Add a dummy class-default level at the top of the policy and apply the shaper as a child policy of this class.

- CSCud58793

  Symptom: The FPD version is blank

Conditions: Upgrade to the new firmware rev. and a subsequent switchover. Occurs when you upgrade the router to a new firmware version and issue an RSP switchover.

Workaround: Reloading the RSP can resolve the issue.

- CSCud60410

  Symptom: The router drops EFP traffic.

  Conditions: Occurs when you add a new EFP to an existing bridge domain interface (BDI) while running L3 multicast.

  Workaround: Issue a **shutdown/no shutdown** on the Ethernet interface and issue the **clear ip mroute** command.

- CSCud61931

  Symptom: As OC-3 interface module controller does not become active using loopback local.

  Conditions: Occurs with the A900-IMA4OS interface module when there is no SFP inserted in the port.

  Workaround: Insert an SFP in the appropriate port.

- CSCud64347

  Symptom: The router creates a data loop when using a REP VLAN load balancing configuration.

  Conditions: Occurs with a REP VLAN load balancing configuration when a bridge-domain is bound to a VPLS VC.

  Workaround: None; remove the VLAN load balancing configuration.

- CSCud64923

  Symptom: OSPF connections flap.

  Conditions: Occurs when you configure OSPF between an EVC bridge domain interface (BDI) and a trunk EFP bridge domain interface (BDI) using a port-channel trunk.

  Workaround: There is no workaround.

- CSCud65779

  Symptom: The router does not update the Rx value for C2, J1, and S1S0 bytes.

  Conditions: Occurs when you configure overhead bytes on OC-3 connections.

  Workaround: There is no workaround.

- CSCud65935

  Symptom: End to end ATM ping does not work.

  Conditions: Occurs when you configure a different set of VPI/VCI on either end of an ATM layer 2 circuit.

  Workaround: Configure the same VPI/VCI values on both sides of the connection.

- CSCud71546

  Symptom: The ten Gigabit Ethernet interface drops traffic for 7 seconds following a stateful switchover (SSO).

  Conditions: Occurs when the configuration contains static routes to the destination.

  Workaround: There is no workaround.

- CSCud76209

  Symptom: The OC-3 interface module goes into an out of service state.

Conditions: Occurs when you repeatedly perform an interface module reset (OIR) on the OC-3 interface module.

Workaround: There is no workaround.

- CSCud76679

  Symptom: The router displays a serial interface in the mroute table but does not forward traffic over the assigned interface.

  Conditions: Occurs when you enable multicast traffic on the OC-3 interface module.

  Workaround: There is no workaround.

- CSCud83069

  Symptom: End-to-end traffic does not flow for ATM PVP Mode.

  Conditions: Occurs when you enable ATM PVP Mode.

  Workaround: There is no workaround.

- CSCud83698

  Symptom: Links on the Gigabit Ethernet interface do not become active.

  Conditions: Occurs on the Gigabit Ethernet interface when the local interface is configured for autonegotiation and the remote interface is configured for a speed of 10 Mbps or 100 Mbps.

  Workaround: Toggle the auto-negotiation configuration on the Gigabit Ethernet interface.

- CSCud91892

  Symptom: Remote LFA converges slowly and the router does not learn backup paths for global prefixes.

  Conditions: Occurs when you configure remote LFA with a high number of global prefixes.

  Workaround: There is no workaround.

- CSCue00332

  Symptom: BFD connections flap, bringing down IGP.

  Conditions: Occurs when you enable BFD on an interface that is flapping.

  Workaround: There is no workaround.

- CSCue03418

  Symptoms: The router displays OSPF protocol flaps causing a 20–30 second traffic loss.

  Conditions: The issue occurs very intermittently on a HA system with a 6 second dead-interval value when you issue the **redundancy force-switchover** command;

  Workaround: Increase the dead-interval value.

Open Caveats—Cisco IOS XE Release 3.8(0)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.8(0)S.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

  Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

  Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCty70119

  Symptom: Port shaper rate changes do not take effect.

  Conditions: Occurs when QoS policies attached to EVCs on an interface do not include a shaper configuration; the issue does not occur on EFP policies that include a shaper in a class.

  Workaround: Include a shaper in one class of the EFP policy.

- CSCua39109

  Symptom: The router displays the following console error message:
  `%FMFP_ACL-3-ACL_OBJECT_DOWNLOAD: SIP0: fman_fp_image: ACL create/modify for ACL test9 fail to download because Cannot allocate memory.`

  Conditions: Occurs when the router is running a configuration containing a high number of ACLs.

  Workaround: There is no workaround.

- CSCua55522

  Symptom: The router experiences intermittent flapping on REP segments.

  Conditions: Occurs under the following conditions:

  - An lsl-age-timer is configured
  - The configuration contains multiple REP segments
  - The router is experiencing high CPU utilization.

  Workaround: There is no workaround. However, the following can limit the issue:

  - Limiting the configuration to a single REP segment
  - Using an **lsl-age-timer** of greater than 500 milliseconds

- CSCua62029

  Symptom: The router crashes.

  Conditions: Occurs when you configure a service policy with two child policies with the same name.

  Workaround: Create a child service policy with a different name.

- CSCua73104

  Symptom: The router does not increment QoS port shaper policy counters displayed by the show policy interface command.

  Conditions: Occurs when you configure -A class-default policy on a physical interface -A class-based policy on an EVC interface

Workaround: There is no workaround; however, the router applies the QoS policy normally.

- CSCua77688

  Symptom: The router experiences remote CFM MEP flapping.

  Conditions: Occurs when the router is connected via a CFM xconnect and the link is running a high traffic rate.

  Workaround: Reduce the rate of traffic.

- CSCua90879

  Symptom: QoS policies with a police statement on the class-default class do not take effect.

  Conditions: Occurs when you apply a police statement to the class-default class within a QoS policy on an ingress EVC interface.

  Workaround: Apply the police statement to a static class, such as class cos0.

- CSCub50477

  Symptom: The router does not pass Multicast traffic after a stateful switchover (SSO).

  Conditions: Occurs when you issue an SSO while the router is passing Multicast traffic on an inbound MLP interface.

  Workaround: There is no workaround.

- CSCub65096

  Symptom: The router crashes when running multicast traffic.

  Conditions: Occurs when the router is passing IGMP join messages at a rate of 6 packets per second over 240 serial interfaces.

  Workaround: Send IGMP joins at a lower rate.

- CSCub77354

  Symptom: An RSP switchover causes the serial interfaces to flap on the peer device.

  Conditions: Occurs when you perform an RSP switchover by physically removing the active RSP.

  Workaround: Use the following workarounds:

  - Perform an RSP switchover using the **redundancy force-switchover** command.
  - Configure the local device to use **clock source line** and the remote device to use **clock source internal**.

- CSCub78861

  Symptom: Following a reload, the router handles CFM only on 128 VLANs or bridge-domains.

  Conditions: Occurs when the router configuration contains CFM and more than 128 VLANs or bridge-domains.

  Workaround: There is no workaround.

- CSCuc01154

  Symptom: The router does not report B1, B2, and B3 alarms at normal thresholds.

  Conditions: Occurs on the OC-3 interface module when the router sends errored frames.

  Workaround: There is no workaround.

- CSCuc02617

  Symptom: The router stops passing MPLS LDP traffic.

Conditions: Occurs on MPLS over POS interfaces when the router is sending traffic above the line rate.

Workaround: Send MPLS LDP traffic below the line rate.

- CSCuc23610

  Symptom: The router does not pass IP traffic with an MPLS LDP tunnel label of Imp-null.

  Conditions: Occurs when the router is switching traffic using IP fast-reroute (FRR).

  Workaround: Configure the **mpls ldp explicit-null** command.

- CSCuc44701

  Symptom: FP init fails on reload with TEFP QoS configs

  The router displays an error message similar to the following: `Oct  1 12:07:21.806 IST: %CMRP-3-CHASSIS_MONITOR_READY_TIME_EXCEEDED: R1/0: cmand:  Reloading F1 because it has failed to become ready for packet processing`

  Conditions: Occurs when you reload the router while running a configuration that contains

  – An egress QoS policy attached to a trunk EFP

  – An **encapsulation dot1q** statement within the QoS policy that specifies a large range

  Workaround: There is no workaround.

- CSCuc55739

  Symptom: The console displays an error message similar to the following example:

  `(Oct 8 10:46:53.126 IST: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: SIP1: fman_fp_image: frr 0x200005ab download to CPP failed).`

  Conditions: Occurs following a stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCuc57939

  Symptom: The router stops passing traffic for more than 8 seconds.

  Conditions: SSO Occurs when you initiate a stateful switchover (SSO) with a remote Loop Free Alternate Fast Reroute (LFA FRR) configuration.

  Workaround: There is no workaround.

- CSCuc58371

  Symptom: Some links do not become active on the OC-3 interface module.

  Conditions: Occurs on the OC-3 interface module (IM) configured at a high scale after you perform a multiple soft OIRs on the IM. The issue occurs frequently with SONET framing.

  Workaround: You can use the following workarounds:

  – Apply a **shutdown/no shutdown** to the OC-3 controller.

  – Re-apply the PDH configuration.

  – Add and remove a loopback configuration on the PDH.

  – Add and remove a loopback configuration on the OC-3 controller.

- CSCuc62049

  Symptom: OSPF/BFD interfaces flap when you apply a test access list.

  Conditions: Occurs when you configure an IP ACL on an EVC interface.

  Workaround: Remove the configuration.

- CSCuc66393

  Symptom: The router loses OC-3 interface configurations after an ISSU upgrade.

  Conditions: Occurs on OC-3 serial and POS interfaces after an ISSU software upgrade.

  Workaround: There is no workaround.

- CSCuc68699

  Symptom: The displays a segmentation fault error at cgmu_nq_ccm_convert and crashes.

  Conditions: Occurs when you perform the following actions:

  – Remove QoS policies from an EFP interface

  – Remove policy-maps and class-maps associated with the QoS policy.

  Workaround: There is no workaround.

- CSCuc80957

  Symptom: The router crashes.

  Conditions: Occurs when you rest the 10 gigabit Ethernet interface module (IM) on a non-redundant system using the **hw-module subslot reload** command.

  Workaround: Administratively shut down the IM before resetting the IM.

- CSCuc81334

  Symptom: The router selects a clock source attached to standby RSP.

  Conditions: Occurs after a stateful switchover (SSO).

  Workaround: Remove and restore the clock source configuration.

- CSCuc83088

  Symptom: The router drops traffic during stateful switchover (SSO).

  Conditions: Occurs when the router is running HSRP or VRRP; the issue only occurs when the destination MAC address is a virtual MAC (vMAC) address.

  Workaround: Change the traffic priority and detour traffic prior to the SSO.

- CSCuc87791

  Symptom: The router selects a network clock source before the wait-to-restore timer has expired.

  Conditions: Occurs under the following conditions:

  – A clock source fails, triggering the wait-to-restore timer (which specifies how long the before including a restored clock source in the clock selection process.

  – The clock source becomes active and fails a second time before the wait-to-restore time has passed.

  Workaround: There is no workaround; in some cases you can clear the issue by removing and restoring the clock source configuration.

- CSCuc90006

  Symptom: When you shut down a link within an Multiservice Transport Platform (MSTP) instance, interfaces in other MSTP instances are blocked.

  Conditions: Occurs when the interface in the MSTP instance is the root port.

  Workaround: There is no workaround.

- CSCuc92350

  Symptom: A connection between two copper SFPs does not become active.

  Conditions: Occurs when two SFP interfaces are connected with one side set to 100 Mbps and the other side set to **negotiation auto**.

  Workaround: Set the speed to 10Mbps at both sides, then configure negotiation auto on one side of the connection.

- CSCuc93895

  Symptom: The router has an Automatic Protection Switching (APS) switchover time of more than 1 second.

  Conditions: Occurs on MLPPP interfaces configured at a high scale when the router is running with ICRM in SONET mode.

  Workaround: There is no workaround.

- CSCuc93985

  Symptom: The router initiates an Automatic Protection Switching (APS) switchover during a high availability (HA) stateful switchover (SSO).

  Conditions: Occurs during an HA SSO with single router APS (SR-APS).

  Workaround: There is no workaround.

- CSCuc95716

  Symptom: FPGA software for the OC-3 interface module is not bundled with the XE 3.8 image.

  Conditions: Occurs when upgrading FPGA on the OC-3 interface module.

  Workaround: Manually upgrade the OC-3 FPGA.

- CSCud01644

  Symptom: The active forwarding processor (FP) is on the standby route switch processor (RSP).

  Conditions: Occurs when you boot the two RSPs in quick succession and the FP on the standby RSP becomes active before the FP on the active RSP.

  Workaround: Reload the router.

- CSCud01908

  Symptom: The **show platform software object-manager fp active statistics** command shows pending objects on the Forwarding Manager (FMAN) on the forwarding processor (FP), indicating a failure to download configurations from the Route Switch Processor (RSP) to the data plane (DP).

  Conditions: Occurs when you apply a QoS shaping configuration at a high scale.

  Workaround: There is no workaround.

- CSCud04407

  Symptom: The router displays the following console error message: `Error - packet with unsupported linktype 3`

  Conditions: Occurs when the router is passing traffic over the OC-3 interface module.

  Workaround: There is no workaround.

- CSCud04529

  Symptom: The router shows traffic loss.

Conditions: Occurs when the primary path is recovered via remote Loop Free Alternate Fast Reroute (LFA FRR).

Workaround: There is no workaround.

- CSCud06744

  Symptom: The router does not download MPLS global prefixes.

  Conditions: Occurs under the following conditions:

  – You configure Loop Free Alternate Fast Reroute (LFA FRR) at a high scale.

  – The primary or backup paths flap multiple times.

  Workaround: There is no workaround.

- CSCud06772

  Symptom: IPv6 neighbor discovery does not function properly after stateful switchover (SSO); the router loses traffic and eventually recovers.

  Conditions: Occurs with IPv6 traffic after stateful switchover (SSO).

  Workaround: Configure software BFD sessions.

- CSCud07642

  Symptom: The ASR 903 is unable to pass traffic to the ASR 9000.

  Conditions: Occurs with a clear-channel ATM over MPLS configuration using AAL0 encapsulation.

  Workaround: Enable MPLS control-word on the ASR 9000.

- CSCud12587

  Symptom: When handling IS-IS packets, the router punts the traffic to the Route Switch Processor (RSP) and applies policing to limit the traffic to 1 Mbps.

  Conditions: Occurs when you enable IS-IS over an Ethernet over MPLS (EoMPLS) connection.

  Workaround: Use IS-IS over another connection type or limit the IS-IS traffic to less than 1 Mbps.

- CSCud13242

  Symptom: The ASR 903 does not display an alarm when nV satellite authentication fails.

  Conditions: Occurs when the ASR 9000 and ASR 903 are in an nV satellite configuration and the routers are configured with a different serial-number value.

  Workaround: There is no workaround.

- CSCud13535

  Symptom: The router drops imposition traffic sent to a neighbor device over a VPLS pseudowire.

  Conditions: Occurs when the neighbor device configuration includes the **no split horizon group** command.

  Workaround: Remove the **no split horizon group** command from the VPLS neighbor device.

- CSCud15785

  Symptom: The router experiences flaps in REP traffic.

  Conditions: Occurs when the MAC limit feature is configured at a high scale.

  Workaround: Disable the MAC limiting feature.

- CSCud24648

Symptom: The router standby RSP displays an ether_efp_cfg_message_unmarshal_ error message and crashes.

Conditions: Occurs under the following conditions:

- The router has an 8 port Gigabit Ethernet interface module (IM)
- The IM is configured with a service instance
- The service instance has an xconnect and bridge domain interface (BDI) configuration
- You perform an soft OIR (reset) on the IM while the standby RSP is booting

Workaround: Wait for the standby RSP to boot before resetting the IM.

- CSCud26382

  Symptom: The router drops traffic on an EFP interface after you perform a stateful switchover (SSO).

  Conditions: Occurs under the following conditions:

  - You boot the standby RSP
  - The router configuration contains an EFP interface on a Gigabit Ethernet port and a bridge domain interface in a down state.
  - After the router reaches an SSO state, you issue a no shutdown command on the peer router to bring the EFP interface up.
  - You perform an stateful switchover (SSO) on the router.

  Workaround: Issue a shutdown/no shutdown on the gigabit Ethernet port.

- CSCud26997

  Symptom: The IOMD process can crash on the T1/E1 interface module.

  Conditions: Occurs during RSP switchover with a configuration containing CEM, ATM, IMA layer 2 attachment circuits, and pseudowires.

  Workaround: There is no workaround.

- CSCud28553

  Symptom: The router stops passing Switch Port Analyzer (SPAN) traffic.

  Conditions: Occurs after you apply a **shutdown/no shutdown** on the SPAN source port with Ethernet flow point (EFP) and bridge domain interface (BDI) configurations.

  Workaround: Enable and disable the SPAN session

- CSCud28685

  Symptom: Ping fails between the CE1 and CE2 devices when the ASR 903 is acting as the PE device.

  Conditions: Occurs when the SONET controller or ATM interface experiences an interface flap.

  Workaround: Perform a soft OIR on the interface module.

Resolved Caveats—Cisco IOS XE Release 3.8(0)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.8(0)S.

- CSCty41692

  Symptoms: Standby PRE crashes when you add an IPV4 VRF AF on the active PRE. The issue does not occur on the active PRE.

  Conditions: Occurs when you remove and re-apply a configuration when BGP is in read-only mode.

  Workaround: Once BGP exits read-only mode, this issue will not happen.

- CSCty85926

  Symptoms: The VC (VPLS/EoMPLS) stays down and displays the following message in the **show mpls l2 vc detail** command: `Signaling protocol: LDP, peer unknown`

  Conditions: Occurs if you configure LDP GR; do a SSO switchover and configure the VC after the switchover is complete.

  Workaround: There is no workaround; reload the switch.

- CSCtz96504

  Symptoms: Backup VCs remain down after SSO.

  Conditions: Occurs at high scale, such as when you create 500 primary and 500 backup VCs.

  Workaround: You can use the **clear xconnect peerid** *peerid of the PW* **vcid** *vcid* command to bring the backup VCs to an SB state; however, this is not usually recommended.

- CSCtz98347

  Symptoms: When IS-IS is configured to run level-2, IS-IS LFA does not create repair path if the total metric to a prefix is 1024.

  Conditions: Seen with 15.2(2)S and when the IS-IS metric is more than 1024 and configured with level-2.

  Workaround: Ensure the total metric to a prefix is less than 1024, or use narrow metric setting

- CSCua27852

  Symptoms: Traffic loss is seen in pure BGP NSR peering environment.

  Conditions: The symptom is seen on a Cisco router that is running Cisco IOS Release 15.2(2)S, and the BGP peerings to CEs and RR are all NSR-enabled.

  Workaround: Enable the **bgp graceful-restart** command for RR peering.

- CSCua61330

  Symptoms: Traffic loss is observed during switchover if BGP graceful restart is enabled or the next hop is learned by BGP.

  Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCua66870

  Symptoms: When changing RPF neighbor (S,G) in PIM-dense mode, OIF on (*,G) is pruned unexpectedly.

  Conditions: Occurs when you use PIM-dense mode.

  Workaround: There is no workaround.

- CSCub61344

  Symptom: Link Control Protocol (LCP) negotiation fails, causing an MLP bundle to stop passing traffic.

  Conditions: Occurs under the following conditions:

  - The router is configured with a T1 interface on the OC-3 interface module (IM)
  - The OC-3 interface module uses SONET framing
  - The T1 serial interface is part of an MLP bundle
  - You change the CRC configuration value of the MLP bundle

  Workaround: Follow these steps:

  - Remove the T1 interface from the MLP bundle.
  - Perform a soft OIR (IM reset) on both ends of the connection.
  - Wait for the T1 interface to become active.
  - Add the T1 interface back into the MLP bundle.

- CSCud04161

  Symptom: The router incorrectly displays a CFM Delay Measurement Message (DMM) value of 0.

  Conditions: Occurs under any of the following conditions:

  - You dynamically add a member link to a port-channel.
  - You issue a shutdown/no shutdown on a member link of a port-channel.

  Workaround: Wait for PTP to synchronize before configuring DMM scheduling.

Restrictions and Caveats in Cisco IOS XE 3.9 Releases

This chapter provides information about restrictions and caveats in Cisco IOS XE 3.9 releases.

Note We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

This chapter contains the following sections:

Limitations and Restrictions

The following limitations apply to the Cisco ASR 903 Router in IOS XE Release 3.9(0)S and later:

TDM Limitation

- The **configure replace** command is not supported for TDM interfaces.

ATM IMA Limitation

- You can create a maximum of 16 IMA groups on each T1/E1 interface module.

Bidirectional Forwarding Detection Limitations

- The minimum supported timer value for software-based BFD sessions is 200 ms x 3 (using a multiplier of 3). The router supports up to 64 offloaded BFD sessions using a 200 ms x 3 timer.
- The Cisco ASR 903 Router supports hardware offloading of BFD echo mode packets for up to 255 sessions. The router handles additional BFD echo mode sessions in software.

Note You cannot convert more than 255 normal BFD sessions to echo mode BFD sessions; the router reaches the offload limit and you must remove and reconfigure the remaining sessions.

- The minimum supported timer value for offloaded BFD echo mode sessions is 3.3 ms.

- In Release 3.9, the router keeps hardware and software-handled BFD echo mode sessions active during ISSU. Releases prior to 3.9 do not maintain hardware-offloaded BFD echo mode sessions during ISSU.
- If you downgrade from 3.9 to a prior release with a BFD echo mode configuration, you must increase the timer to 200ms or greater.

Bridge Domain Interface Limitation

- The **mtu** command is not supported on BDI interfaces; however the **ip mtu** command is supported.

Clocking and Timing Limitations

- Only a single clocking input source can be configured within each group of eight ports (0-7 and 8-15) on the T1/E1 interface module using the network-clock input-source command.
- Synchronous Ethernet clock sources are not supported with PTP. Conversely, PTP clock sources are not supported with synchronous Ethernet. However, you can use hybrid clocking to allow the router to obtain frequency using Synchronous Ethernet and phase using PTP.
- PTP over Ethernet is not supported in multicast mode; only unicast mode is supported
- G.8265.1 telecom profile is not supported for PTP over Ethernet.
- The Cisco ASR 903 Router does not support a mix of IPv4 and Ethernet clock-ports when acting as a transparent clock or boundary clock.
- Out-of-band clocking and the **recovered-clock** command are not supported.
- The Synchronization Status Message (SSM) is not currently on OC-3 and OC-12 interfaces.
- End-to-end Transparent Clock is not supported for PTP over Ethernet.

Dying Gasp Limitations

The Cisco ASR 903 Router supports dying gasp under the following scenarios:

- Ethernet OAM is disabled
- Interface is shut down
- Interface enters error-disabled state
- Router reload
- Dying Gasp is not supported in the event of a power failure.

EFP Limitations

- Trunk EFPs are not supported on port channel interfaces.
- Up to 1000 VLANs are supported for trunk EFP over etherchannel traffic.

Ethernet IM Limitations

- The Cisco ASR 903 Router does not support the Facilities Data Link (FDL) on Ethernet interfaces.
- The Cisco ASR 903 Router does not support the **mac-address** command on Gigabit Ethernet interface modules.
- 10 Gigabit Ethernet interface modules are not supported in slots 4 and 5.
- When you install a Gigabit Ethernet IM in the topmost interface module slot (slot 5), the last interface (interface GigabitEthernet0/5/0) is not operational; the port is reserved for internal communication.

- When you configure the copper and SFP Gigabit Ethernet interface modules on a router with redundant RSPs, the **speed** and **duplex** commands are not visible in interface configuration mode until you apply a **shutdown/no shutdown** to the interface.
- Fragmentation is not supported with Multicast traffic.
- The SFP-GE-T module supports only 100 Mbps and 1000 Mbps speeds.
- Load balancing using an odd number of port-channel member links is not supported.

IP Multicast Limitation

- Bandwidth-Based Call Admission Control (CAC) feature is not supported.

IPv6 Limitations

The following limitation applies when using IPv6 on the Cisco ASR 903 Router:

- IPv6 Neighbor Discovery (ND) cache timer expiry is 4 hours. To prevent the neighbour adjacency from being deleted after the timer expires:
  - configure hardware based BFD sessions with the neighbours, or
  - configure static IPv6 neighbours, or
  - configure the **ipv6 nd cache expire timer refresh** command.

IS-IS Limitations

- IS-IS over IPv6 is not supported on VRF instances.
- Only one IS-IS process is permitted when you configure IS-IS with the **address-family ipv6** and **bfd-all-interfaces** commands.
- The IS-IS total and per-stream convergence time increases as the number of prefixes increases.
- The Cisco ASR 903 Router supports up to 3000 IS-IS nodes.

MLPPP Limitations

The following limitations apply when using MLPPP on the Cisco ASR 903 Router:

- All links in an MLPPP bundle must be on the same interface module.
- All links in an MLPPP bundle must be of the same bandwidth.
- The Cisco ASR 903 Router supports a maximum of 16 links per bundle
- To change the MLPPP bundle fragmentation mode between enabled and disabled, perform a **shutdown/no shutdown** on the bundle.
- LFI is not supported
- Multiclass MLP is not supported
- The Cisco ASR 903 Router supports MLPPP statistics with the following limitations:
  - Packet counters on the bundle display the number of fragments rather than packets.
  - Control packets are accounted on the bundle.
- If you increase the maximum transmission unit (MTU) size on an MLPPP interface to a value higher than the maximum received reconstructed unit (MRRU) value on the peer interface, this can bring the MLPPP tunnel down. To restore the tunnel, perform a shutdown/no shutdown on the interface.

MPLS VPN Limitation

- MPLS VPN (L3VPN) Fragmentation does not function properly if an access interface has a higher MTU value than a core interface. To ensure that fragmentation functions correctly, configure the core interface MTU with a value that exceeds the access interface MTU and relevant headers.

OC-3 IM Limitations

- The **configure replace** command is not supported on the OC-3 IMs.
- MPLS-TP is not supported over POS interfaces.
- Multicast is not supported on OC-12 interfaces.
- DS0 channelization is not currently supported.
- MPLS is supported only on PoS interfaces; MPLS on T1/E1 links is not supported.
- IP-FRR and BFD-triggered FRR are not supported on MPLS over POS links.
- Fragmentation is not supported with Multicast traffic on PoS interfaces.
- QoS is not supported for Multicast traffic on PoS interfaces.
- QoS is supported on POS interfaces on optical interface module.
- Three-level QoS policies are not supported on OC-3/OC-12 serial, MLPPP, and PoS interfaces. You can only apply two-level QoS policies.
- The Synchronization Status Message (SSM) is not currently on OC-3 and OC-12 interfaces.

Pseudowire/AToM Limitation

- The Cisco ASR 903 Router supports ATM over MPLS N-to-one cell mode for a single ATM Virtual Channel Connections (VCCs) or Permanent Virtual Circuits (PVCs) to a pseudowire, but does not support mapping to multiple VCCs or PVCs.
- The Cisco ASR 903 Router does not support ATM over MPLS one-to-one cell mode.
- The Cisco ASR 903 Router supports pseudowire ping using the CW method; pseudowire ping using the TTL method is not supported.
- The Cisco ASR 903 Router supports a maximum of 2000 pseudowires in any combination.
- The following features are not currently supported on pseudowire connections:
  - Ethernet VLAN to Ethernet VLAN L2VPN interworking (bridged and routed modes)
  - Ethernet VLAN to ATM AAL5 L2VPN Interworking (bridged and routed modes)

The following pseudowire (PW) features are not supported over MPLS-TP connections:

- ATM OAM Cell Emulation for ATM AAL5 over MPLS on PVC and in VC Class.
- BFD / VCCV over ATM AC over MPLS TP
- Ethernet port to ATM AAL5 PVC L2VPN Interworking (bridged and routed modes)
- MIB support including PW-TDM-MIB, PW-ATM-MIB, and PW-CESOPSN-MIB
- N:1 PVC Mapping with non-unique VPI (N>1)

QoS Limitations

For a description of QoS features and limitations on the Cisco ASR 903 Router in Release 3.9S, see http://www.cisco.com/en/US/docs/routers/asr903/software/guide/chassis/Release3.9.0S/ASR903-Chassis-SW-39.html

Software Upgrade Limitation

We recommend you set the **interface-module-delay** value to 150 or greater in order to ensure sufficient time for IM software upgrades.

Subinterfaces Limitation

The Cisco ASR 903 Router does not support subinterface configurations except on ATM interfaces.

You can configure similar functionality using multiple Ethernet Virtual Connections on an interface. For more information, see Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.

T1/E1 IM Limitations

- Inverting data on the T1/E1 interface is not supported—Inverting the data stream using the invert data interface command is not supported.
- Bit error rate test (BERT) patterns have limited support—Currently, only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported for BERT.
- If you issue the **no card type** command on the controller, you must reload the router in order to configure a new **card type** value.

Caveats in Cisco IOS XE 3.9S Releases

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in this chapter.

This section describes caveats in Cisco IOS XE 3.9S releases. The following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

The following sections describe the open and resolved caveats in 3.9S Releases:

- Open Caveats—Cisco IOS XE Release 3.9(2)S, page 6
- Resolved Caveats—Cisco IOS XE Release 3.9(2)S, page 6
- Open Caveats—Cisco IOS XE Release 3.9(1a)S, page 14
- Resolved Caveats—Cisco IOS XE Release 3.9(1a)S, page 18
- Open Caveats—Cisco IOS XE Release 3.9(0)S, page 27

- Resolved Caveats—Cisco IOS XE Release 3.9(0)S, page 31

Open Caveats—Cisco IOS XE Release 3.9(2)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.9.2S.

- CSCue20035

  Symptom: Virtual circuit (VC) status goes down after reload.

  Conditions: This issue occurs when reloading the core side trunk EFP BDI with port channel using cross connect. LDP comes up but VC status goes down.

  Workaround: On core side, use EVC bridge-domain BDI with port channel instead of trunk EFP BDI with port channel.

- CSCue67267

  Symptom: High traffic drop on Stateful Switchover (SSO). Double dip on SSO.

  Conditions: This issue occurs occasionally (one in five iterations) on Cisco ASR 903 Router with MVPN scale setup.

  Workaround: There is no workaround.

- CSCuf89283

  Symptom: Connectivity Fault Management (CFM) sessions configured on pseudowire continue to flap.

  Conditions: This issue occurs when route flaps quick enough to prevent bringing down of the pseudowire.

  Workaround: Bring down the pseudowire and bring it back up again.

- CSCuh94841

  Symptom: 10 Gigabit Ethernet interface flaps without trigger causing traffic to switch to protected label-switched path (LSP).

  Conditions: This issue occurs when the script is run for continuous SSO.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.9(2)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.9.2S.

- CSCud61551

  Symptom: Serial Number of the RSP in slot 1 does not display in the **show inventory** command output.

  Conditions: This issue occurs under unknown conditions.

  Workaround: Reload the router.

- CSCue29865

  Symptom: Values do not display for OC-12 mode after shutting the IM bay.

  Conditions: This issue occurs after shutting the IM bay. Values are not displayed for OC-12 mode, but the values are displayed for the Gigabit Ethernet card.

Workaround: There is no workaround.

- CSCue32016

  Symptom: On IM online insertion and removal (OIR) or Router reload with shutdown on CE controller, Ethernet (core) does not transmit any packets.

  Conditions: This issue occurs when remote peer does not assert alarm indication signal (AIS) downstream.

  Workaround: There is no workaround.

- CSCue44876

  Symptom:

  - Packet-over-SONET (PoS) interface on the high availability (HA) system continues flapping
  - Complete traffic is dropped
  - PoS interface of the remote Cisco ASR 903 Router remains in up or down state.

  Conditions: This issue occurs on activating SSO after an IM OIR when configuring PoS interface in OC-12 mode.

  Workaround: There is no workaround.

  More Info: This issue is not seen in OC-3 mode.

- CSCue61850

  Symptom: Maintenance End Points (MEPs) start flapping when **no shutdown** command is issued on EVC bridge-domain (BD) or port channel interface running CFM.

  Conditions: This issue occurs when more than 256 CFM sessions are configured.

  Workaround: Configure fewer CFM sessions (50 to 100).

- CSCue67835

  Symptom: OSPF flaps when you set the dead interval timer as 6 seconds and hello interval as 2 seconds.

  Conditions: This issue is observed when you perform an SSO.

  Workaround: Use the default OSPF hello timers.

- CSCue69818

  Symptom: The **show inventory** command displays a wrong serial number.

  Conditions: Inventory is managed by the "main serial number". However, when using the **show inventory** command for Redundant Power System (RPS) and IM, "PCB serial number" is displayed instead of the "main serial number".

  Workaround: Use the **show diag all eeprom detail** command to list the correct serial number.

- CSCue75372

  Symptom: Time-Hog traceback seen after router or IM reloads.

  Conditions: This issue occurs on bootup of IM or router.

  Workaround: There is no workaround.

- CSCue97180

  Symptom: The Cisco ASR 903 Router sometimes crashes when used as a multicast VPN (mVPN) Encap PE Router.

Conditions: This issue occurs in an mVPN network on exceeding core multicast distribution tree (MDT) scale of 1K with more than 20 virtual routing and forwarding (VRFs) on a flap access interface of a PE Router.

Workaround: Do not exceed more than 1K core MDT scale Work around for a crash is unavailable.

- CSCuf02007

  Symptom: Continuous SEMHOG is seen on the router console with incremental sync failure and IOMD crashes on OC-3 IM.

  Conditions: Router receives continuous SEMHOG for multiple processes.

  Workaround: There is no workaround.

- CSCuf06001

  Symptom: When TCAM limit is reached, statistics do not work accurately.

  Conditions: This issue occurs when the TCAM entries exceed the limit during dynamic modification of service-policy.

  Workaround: There is no workaround.

- CSCuf43992

  Symptom: The router crashes if you configure local span.

  Conditions: This issue is observed when you configure local span on the router.

  Workaround: Use another Encapsulated Remote Switched Port Analyzer (ERSPAN) configuration to work as local span with source and destination ERSPAN session configured in one router.

- CSCuf45656

  Symptom: Cisco ASR 903 Router crashes with segmentation fault.

  Conditions: This issue occurs during multicast convergence on EFP's configured with split horizon.

  Workaround: There is no workaround.

- CSCuf53527

  Symptom: Class of Service (CoS) inner value gets copied into the CoS value.

  Conditions: This issue occurs when configuring Q-in-Q without rewrite service instance.

  Workaround: To ensure CoS inner value does not get copied, apply QoS policy-map.

- CSCuf65301

  Symptom: Micro flaps observed on the router.

  Conditions: This issue is seen when system is kept idle for hours.

  Workaround: There is no workaround.

- CSCuf79397

  Symptom: F1 is stuck in init state after the standby RSP reloads.

  Conditions: This issue occurs on a reload or OIR of the standby RSP.

  Workaround: Reload the standby RSP again.

- CSCuf81085

  Symptom: After you use the **shutdown** and **no shutdown** commands on the controller of PE, IMA VCs go down.

  Conditions: This issue is observed after using the **shutdown** and **no shutdown** commands on the OC3 controller on PE routers.

Workaround: Use the **shutdown** and **no shutdown** commands on the controller.

- CSCuf89767

  Symptom: When IGMP snooping is enabled, multicast traffic is not accurately filtered. Layer 3 multicast traffic floods all ports of the bridge-domain.

  Conditions: This issue occurs when start-up configuration includes port channels along with TEFP/EFP as part of the bridge-domain.

  Workaround: There is no workaround.

- CSCug05239

  Symptom: Traffic drops on the router.

  Conditions: This issue occurs when configuring multichassis Link Aggregation Control Protocol (MLACP) switchover with Ethernet over Multiprotocol Label Switching (EOMPLS).

  Workaround: Configure port channel with EOMPLS.

- CSCug10116

  Symptom: Traffic and ping do not flow through ATM interfaces on multiple controllers.

  Conditions: Series of **shutdown** and **no shutdown** commands on the controller or interface lead to the failure.

  Workaround: There is no workaround. To recover from failure, perform an IM OIR.

- CSCug18185

  Symptom: When the interfaces comes up after bootup, traffic received on the Cisco ASR 903 Router serial interfaces are not switched to the BDI connected to Ixia.

  Conditions: This issue occurs when ARP resolution of the Ixia connected interface IP address fails.

  Workaround: Ping the Ixia port connected to the Cisco ASR 903 Router from another router connected to the Cisco ASR 903 Router using Gigabit Ethernet interface.

- CSCug18630

  Symptom: When you perform an OIR on the standby and active RSPs, CMAND crashes.

  Conditions: This issue is observed after performing multiple standby OIRs and bringing the standby machine up.

  Workaround: There is no workaround.

- CSCug21145

  Symptom: When system crashes, sometimes core files are generated with CRC errors.

  Conditions: This issue occurs when the system crashes under stress conditions.

  Workaround: There is no workaround.

- CSCug27073

  Symptom: Multicast replication is improper when 255 outgoing interfaces (OIF's) are configured.

  Conditions: This issue occurs when:

  - Perfuming IM OIR (soft/hard)
  - Clearing MRoutes (sometimes)
  - Enabling/disabling IGMP Snooping

  Workaround: There is no workaround.

- CSCug31414

  Symptom: Multicast traffic drops on changing interface configuration from TEFP to VPLS over port channel (PoCH).

  Conditions: This issue occurs when converting a layer 2 interface to layer 3; and then configuring IP PIM and IP address in quick succession.

  Workaround: Use **shutdown** and **no shutdown** command on the interface.

  More Info: The problem occurs only when the adjacency create notification is received earlier than the convert to layer 3 notification.

- CSCug44762

  Symptom: The POS interface stays down after using the **shutdown** and **no shutdown** commands.

  Conditions: This is issue is observed when you use the **shutdown** and **no shutdown** commands on the POS interface.

  Workaround: Use the **shutdown** and n**o shutdown** commands on the controller.

- CSCug61357

  Symptom: ISIS adjacency and BFD stay down after using the **shutdown** and **no shutdown** commands.

  Conditions: This issue is observed in R-LFA configurations.

  Workaround: Use the **shutdown** and **no shutdown** commands again.

- CSCug63862

  Symptom: When configured, SATOP interfaces does not come up.

  Conditions: This issue occurs on configuring SATOP on the router.

  Workaround: Use IM OIR.

- CSCug74071

  Symptom: When scaling up MPLS-TE tunnels to full scale (512), sometimes the following message is displayed: "%FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: SIP1: fman_fp_image: adj 0x9fdd, Flags Incomplete download to CPP failed".

  Conditions: This issue occurs when MPLS-TE tunnels are scaled to full scale (512) on the router in a single instance.

  Workaround: There is no workaround.

- CSCug83807

  Symptom: Multicast traffic is dropped as TCAM entries are encountered.

  Conditions: This issue occurs when TCAM entries are encountered.

  Workaround: There is no workaround.

- CSCug83842

  Symptom: ATM/IMA path level controllers go down with alarms LP-AIS and T15 LOMF in the Cisco ASR 903 Router.

  Conditions: This issue occurs on either on bootup of the router or OIR of the IM. Along with these alarms, B1/B2 alarms are reported at the controller level. As B1/B2 alarms are high priority alarms, the path level controllers stays down.

  Workaround: Reload IM or use the **shutdown** and **no shutdown** command on the main controllers.

- CSCug84544

  Symptom: POS interface output displays wrong counter values.

  Conditions: This issue occurs when using PPP encapsulation.

  Workaround: There is no workaround.

- CSCug86963

  Symptom: Bidirectional Forwarding Detection (BFD) is unable to resolve neighbor Address Resolution Protocol (ARP).

Conditions: This issue occurs when software BFD is configured with static client; and IM OIR or reload is performed.

Workaround: Use manual ping.

- CSCug91295

  Symptom: UDP based ACLs do not work after a router reload.

  Conditions: This issue occurs after reload.

  Workaround: Remove and add the ACL.

- CSCug96958

  Symptom: Inverse Multiplexing for ATM (IMA) interfaces stay up even when you use the **shutdown** command to shut down the controller.

  Conditions: This issue is observed when you use the **shutdown** command on the OC-3 controller.

  Workaround: Use the **no shutdown** command bring up the controller and interfaces.

- CSCug97639

  Symptom: IPv4 VRF ping fails when disabling IPv6 unicast-routing globally.

  Conditions: This issue occurs when IPv6 unicast-routing is disabled.

  Workaround: Enable IPv6 unicast-routing

- CSCug99750

  Symptom: The Cisco ASR 903 Router crashes when it accesses unpopulated data structures.

  Conditions: This issue is observed when you perform an IM OIR and use the **shutdown** and **no shutdown** commands.

  Workaround: There is no workaround.

- CSCuh00343

  Symptom: Node runs out of memory if node has more 1K pseudowires. Pseudowire can be either Ethernet over MPLS (EoMPLS) or Virtual Private LAN Services (VPLS).

  Conditions: Access instability cause these memory leaks. If network is stable then chances of observing this issue is minimal.

  Workaround: There is no workaround.

- CSCuh06740

  Symptom: Router gets reloaded after performing a soft OIR.

  Conditions: This issue is observed after you perform a soft OIR or subsequent SSOs.

  Workaround: There is no workaround.

- CSCuh16011

  Symptom: FMAN-FP crashes when you perform ab IM OIR.

  Conditions: This issue is observed when you perform multiple IM OIRs with around 65 BFD sessions.

  Workaround: Reload the router.

- CSCuh18073

  Symptom: In a domain with 2 BGP exit points acting in Active or Repair mode, traffic would be exiting the domain through Repair path BGP PE instead of exiting through Active path BGP PE.

  Conditions: This issue occurs in the following conditions:

  - Environment has 2 BGP exit points
  - A change in one of the core links to the primary BGP exit point results in Repair BGP PE becoming Active BGP PE and vice versa

  In this scenario, even after BGP convergence, data packets would traverse through previous primary BGP PE (now repair path PE).

  Workaround: There is no workaround.

- CSCuh18503

  Symptom: BFD IPv6 sessions may not come up between Cisco ASR 9000 and Cisco ASR 903 Routers.

  Conditions: This issue is observed when the packets sent from Cisco ASR 903 Router have invalid UDP checksums.

  Workaround: There is no workaround.

- CSCuh27117

  Symptom: Traffic loss of about six to eight seconds is observed when you perform an SSO.

  Conditions: This issue is observed when you perform the switchover before IM OIR or the interface flaps.

  Workaround: There is no workaround.

- CSCuh33255

  Symptom: Traffic does not flow through most multilink PPP (MLP) interfaces post In-Service Software Upgrade (ISSU).

  Conditions: This issue occurs on HA system performing ISSU or killing IOMD process followed by switchover.

  Workaround: Use **shutdown** and **no shutdown** command on MLP interface to recover the traffic.

- CSCuh59723

  Symptom: On removing one out of the two member links from the MLP bundle, traffic and ping fail.

  Conditions: This issue occurs with T1E1/OC-3 IM when using **shutdown** and **no shutdown** command or when removing cable from one of the member serial interface.

  Workaround: Reload the router.

- CSCuh65426

  Symptom: Circuit emulation (CEM) packets use class default after **shutdown** and **no shutdown** on CEM circuit, with or without QoS policy

  Conditions: After removing and adding QoS policy on CEM circuits, followed by CEM interface flap, CEM packets neither exit with default EXP marking of 5 nor exit with the marking specified in ingress qos policy. This occurs after reloading the router with policies intact on CEM interface and only in the presence of Hot-Standby Psuedo Wires (HSPW).

  Workaround: There is no workaround.

- CSCuh77595

  Symptom: On using **configure replace** command, the standby router crashes.

  Conditions: This issue occurs when replacing the TE tunnel configuration with Startup configuration using **configure replace** command.

  Workaround: There is no workaround.

- CSCuh77762

  Symptom: The TenGigabitEthernet port operates at one gigabit speeds in WAN-PHY mode on Cisco ASR 903 Routers. This leads to a huge amount of output drop.

  Conditions: This issue is observed if a QoS policy is configured on the TenGigabitEthernet interface.

  Workaround: There is no workaround.

- CSCuh86102

  Symptom: The interface stops forwarding traffic.

  Conditions: This issue is observed when the TenGigabitEthernet interface is in WAN-PHY mode and R0 is active.

  Workaround: Use R1.

- CSCuh99117

  Symptom: Cisco ASR903 Router packets drop for some of the prefixes in MPLS network.

  Conditions: This issue occurs when MPLS L3 VPN is configured on Cisco ASR903 Router with MVPN template.

  Workaround: There is no workaround.

- CSCui08269

  Symptom: Error objects are seen and traffic does not flow through HSPW VC's.

  Conditions: This issue occurs on using **do clear mpls ldp ne** command when more than 100 HSPW VC's are configured.

  Workaround: Remove and add the EFP.

- CSCui16418

  Symptom: After SSO, 10 Gigabit Ethernet interface flaps and traffic is dropped.

  Conditions: This issue occurs during SSO switchover on the10 Gigabit Ethernet interface of a HA system.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.9(1a)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.9(1a)S.

- CSCuc33798

  Symptom: IMA links goes down with over subscription traffic.

  Conditions: This issue is seen with over subscription traffic

  Workaround: Use line rate.

- CSCuc42085

  Symptoms: The 1PPS output from the ASR 903 is out of range when compared to the 1PPS output of the PTP master clock.

  Conditions: This issue occurs when the router is configured as a hybrid clock (ordinary/boundary) and there are intermediate hops between the router and the PTP master clock.

  Workaround: There is no workaround.

- CSCue29809

  Symptom: Mismatch in the MIB object entSensorThresholdEvaluation value for CiscoEntitySensorMIB.

  ```
  entSensorThresholdEvaluation.1086.1 = false(2) (value should be true)
  entSensorThresholdEvaluation.1086.2 = false(2) (value should be true)
  ```

  Conditions: This issue occurs in normal working conditions.

  Workaround: There is no workaround.

- CSCue29865

  Symptom: Values do not display for OC-12 mode after shutting the IM bay.

  Conditions: This issue after shutting the IM bay. Values are not displayed for OC-12 mode, but the values are displayed for the Gigabit Ethernet card.

  Workaround: There is no workaround.

- CSCue35103

  Symptom: CPU goes high on executing **show mac-address-table** command.

  Conditions: Scaled MAC entries are learned over BD.

  Workaround: Execute the command with reduced term length.

- CSCue42139

  Symptom: The Precision Time Protocol (PTP) state is stuck in acquiring state.

  Conditions: This issue occurs when the active RSP is removed and the T3 time-stamping is stuck and the PTP stays in acquiring state.

  Workaround: Reload the IM or unconfigure and configure the PTP.

- CSCue63229

  Symptom: IMA interfaces flap frequently every 1530 minutes. The issue does not occur on member links.

  Conditions: This issue occurs when you increase the number of member links in the IMA group to 16.

  Workaround: There is no workaround.

- CSCue67835

  Symptom: OSPF flap with aggressive timers (2sec hello interval, 6sec dead interval).

  Conditions: This issue occurs after performing an SSO.

  Workaround: Use the default OSPF hello timers.

- CSCue75372

  Symptom: Time-Hog traceback seen after router or IM reloads.

  Conditions: This issue occurs on bootup of IM or router.

  Workaround: There is no workaround.

- CSCue87629

  Symptom: INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client “iosd-nile” messages may appear on the console.

  Conditions: This issue occurs when a **shutdown** followed by a **no shutdown** command is executed on the G8032 ring interface of a peer or local device.

  Workaround: There is no workaround.

- CSCue92393

  Symptom: CEM SatoP circuits with the router in Core remain in down state after initial configuration. The **show cem circuit** command output on ASR903 shows that the circuits are down.

  Conditions: This issue occurs when the CEM SatoP circuits are configured using script via tcl and tftp_config. This forces a lot of configuration dump on router console simultaneously. The issue may also be seen after router reload with saved CEM Satop configurations.

  Workaround: Perform a controller **shutdown** followed by a **no shutdown** on OC-3 IM on the router.

- CSCuf05090

  Symptom: Standby IM resets continuously with running configuration synchronization failure.

  Conditions: This issue occurs after a downgrade of all IMs and the IMS are removed from the slot and a upgrade is performed.

  Workaround: Reload the router completely.

- CSCuf35542

  Symptom: PFM is fails for about 5minutes after OIR on the master.

  Conditions: This issue occurs after OIR is performed two times on the master

  Workaround: Wait for 5-6 minutes after the OIR.

- CSCuf79397

  Symptom: F1 is stuck in init state after the standby RSP reloads.

  Conditions: This issue occurs on a reload or OIR of the standby RSP.

  Workaround: Reload the standby RSP again.

- CSCug05491

  Symptom: The router drops traffic on VPLS circuits.

  Conditions: This issue occurs when you take the following actions:

  - Configure REP with VLAN load balancing
  - Configure VPLS VFI on the VLANs
  - Issue an stateful switchover (SSO)

  Workaround: There is no workaround.

- CSCug14420

  Symptom: Traceback observed while performing OIR of IM.

  Conditions: This issue occurs while performing OIR T1E1 IM

  Workaround: There is no workaround.

- CSCug21352

  Symptom: The convergence time is more than 2secs on the router.

  Conditions: This issue occurs when convergence time is more than expected. It takes around 2.5 seconds to converge from Active to backup path with 450 CEM interfaces.

  Workaround: There is no workaround.

- CSCug70182

  Symptom: ASR903 -IMA8S port stays up without inserting a fiber.

  Conditions: This issue is observed when GLC-FE-100FX optic is used

  Workaround: There is no workaround.

- CSCug77786

  Symptom: The router develops false notifications, syslog messages and cefcFRUInserted traps when performing RP card switchover. The false notifications create false alarms in Prime Network.

  Conditions: This issue occurs after RP card switchover on the router.

  Workaround: There is no workaround.

- CSCug81561

  Symptom: Convergence time is more than 50ms with EoMPLS after SSO.

  Conditions: This issue occurs when port channel and BDI configurations exist on the router and SSO convergence time is more than 50ms.

  Workaround: There is no workaround.

- CSCug83807

  Symptom: Multicast traffic is dropped as TCAM entries are encountered.

  Conditions: This issue occurs when TCAM entries are encountered.

  Workaround: There is no workaround.

- CSCug91295

  Symptom: UDP based ACLs do not work after a router reload.

  Conditions: This issue occurs after reload.

  Workaround: Remove and add the ACL.

- CSCug94257

  Symptom: The **show ptp port running detail** command shows the wrong stream id.

  Conditions: This issue occurs under normal working conditions.

  Workaround: Use the **show plat soft ptp** command get the correct stream id.

Resolved Caveats—Cisco IOS XE Release 3.9(1a)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.9(1a)S.

- CSCtw76473

  Symptom: The router displays packet drops on some VPLS pseudowire virtual circuits (VCs) on the disposition side.

  Conditions: Occurs under the following conditions:

  - The core network is running MPLS-TP tunnels
  - There is an SSO switchover on the remote end or an LDP neighbor reset on the peer end.

  Workaround: There is no workaround.

- CSCud09142

  Symptom: Fp active error messages seen when interface tunnel TP is removed when HA is configured.

  Conditions: This issue is seen after removing tunnel TP interface.

  Workaround: There is no workaround.

- CSCud30554

  Symptom: Object download failure messages are displayed on console during object cleanup. This may cause a possible leak in the hardware resource if the objects are not cleaned up.

  Conditions: This issue is seen during the Virtual Circuit deletion.

  Workaround: There is no workaround.

- CSCud42914

  Symptom: Object download messages are observed when default values are se on the MPLS core interface.

  Conditions: This issue occurs when default values are se on the MPLS core interface.

  Workaround: There is no workaround.

- CSCud59242

  Symptom: Traffic stops forwarding for 10-20 groups out of 1000 groups when IGMP snooping is enabled.

  Conditions: This issue occurs when outgoing Layer 2 interface flaps very quickly. This issue occurs when executing the **shutdown** command followed by a **no shutdown** command.

  Workaround: Disable IGMP snooping.

- CSCue10037

  Symptom: After executing the **shutdown** command followed by a **no shutdown** the member link crashes

  Conditions: This issue occurs when CFM Trunk EFP with 256 sessions with an interval of 3.3ms is configured and **shutdown** command followed by a **no shutdown** command is executed.

  Workaround: Configure 50-100 CFM sessions.

- CSCue13187

  Symptom: Duplicate multicast traffic is received after replacing the bridge-domain ID with new bridge-domain ID.

Conditions: This issue occurs when the bridge-domain ID is changed from an existing bridge-domain ID to a new bridge-domain ID.

Workaround: If the bridge-domain needs to be changed, remove the old service instance and configure new service instance with new bridge-domain.

- CSCue15570

  Symptom: Traffic does not resume on a POS interface.

  Conditions: This issue is seen after the router reloads with POS configurations.

  Workaround: Perform the following:

  - Shutdown the interface and then execute a **no shutdown** on the TDM interface
  - Shutdown the controller then execute a **no shutdown** on the TDM controller
  - Soft OIR the OC3 IM.

- CSCue19836

  Symptom: Controller flaps are observed on CE routers with Multirouter Automatic Protection Switching (MR-APS) configured on PE routers with CEM circuits.

  Conditions: This issue occurs when controllers on CE routers flaps when is MR-APS configured on PEs having CEM circuits.

  Workaround: There is no workaround.

- CSCue20607

  Symptom: Port-channel load balances traffic on member-links which are in hot-standby or down state also resulting in traffic blackholes.

  Conditions: This issue is seen when there are redundant member-links which are in hot-standby or down state.

  Workaround: There is no workaround.

- CSCue24854

  Symptom: 70 msec loss is observed after performing an IM OIR in a remote LFA ring.

  Conditions: This issue occurs when doing soft OIR.

  Workaround: Perform a hard OIR for a less than 50 msec loss.

- CSCue34781

  Symptom: The policer in the parent policy-map of an hqos policy attached to an interface stops working after the child policy policer is dynamically modified.

  Conditions: The policy-map attached to the interface is a hierarchical policing policy. Both the child and the parent policy-map have policing actions in their classes. It is seen that the policing in the parent class does not work correctly after the policing action in the child policy is modified dynamically

  Workaround: Remove and re-attach the policy-map on the interface

- CSCue50128

  Symptom: FMFP download failure occurs on reaching 1980 odd number even though 2000 ternary content addressable memory (TCAM) space is allocated for ACLs in the IP template.

  Conditions: This issue occurs in normal conditions when the scale reaches 1980.

  Workaround: There is no workaround.

- CSCue51682

  Symptom: The REP protocol flaps, as indicated by the following error messages:

  ```
  *Feb  8 06:51:38.857: %REP-4-LINKSTATUS: GigabitEthernet0/0/1 (segment 10) is
  non-operational due to neighbor not responding
  *Feb  8 06:51:39.096: %REP-4-LINKSTATUS: GigabitEthernet0/0/1 (segment 10) is
  operational.
  ```

  Conditions: Occurs under the following conditions:

  - The router is sending traffic using the incremental MAC address table
  - Fast LSL is configured using a 200ms timer.
  - The router is configured with more than 2000 MAC addresses.

  Workaround: Remove fast LSL from the REP configuration.

- CSCue54649

  Symptom: Traceback is seen on new active RSP console after performing a SSO.

  Conditions: This issue is seen when OC-3 IM is configured on OC-12 mode. The POS and serial interfaces mayor may not be configured.

  Workaround: There is no workaround.

- CSCue61803

  Symptom: IMs do not get powered off when router is reloaded.

  Conditions: This issue is seen occasionally on reload.

  Workaround: There is no workaround.

- CSCue65149

  Symptom: OBJ messages are observed when changing the interval in EVC BD offload cases (scale).

  Conditions: This issue occurs when 3.3ms session interval and MEPS is configured on the router and then the MEPS and domain configuration is removed and a session interval of 10ms interval is configured.

  Workaround: Configure a low session interval.

- CSCue66137

  Symptom: The IOMD crashes with CPU hog messages.

  Conditions: This issue occurs with OC-3 interface module and traffic is sent over a multilink bundle with packet size greater than 600 byte.

  Workaround: There is no workaround.

- CSCue73478

  Symptom: Standby RSP Sync LED become holdover after switchover.

  Conditions: This issue occurs after a switchover.

  Workaround: There is no workaround.

- CSCue77596

  Symptom: Cos value gets wrongly marked for a QinQ packet

  Conditions: This issue occurs on a service instance with dot1q encapsulation and no rewrite is configured on the interface.The policy map attached in the ingress has marking in it.

  Workaround: There is no workaround.

- CSCue81082

  Symptom: FMAN OBJ download failure seen for (*,G/m) entries on ACL change.

  Conditions: This issue occurs when ACL is configured on the RP and the ACL is deleted or added.

  Workaround: There is no workaround.

- CSCue83621

  Symptom: Policy-map stops working on removing class default class dynamically.

  Conditions: This issue occurs when policy-map is attached to target and class-default of top level is deleted dynamically.

  Workaround: Detach and reattach the policy-map on target.

- CSCue88974

  Symptom: Standby RSP appears as UNKNOWN in **show inventory** command and alarm is raised. The **show facility-alarm** command status reports the alarm.

  Conditions: This issue occurs after OIR is performed on the standby RSP.

  Workaround: There is no workaround.

- CSCue89503

  Symptom: Power supply status become “CRITICAL” after removing or inserting of the power supply.

  Conditions: This issue is seen after multiple OIRs.

  Workaround: There is no workaround.

- CSCue90867

  Symptom: Machine check errors and kernel crash was seen on SSO.

  Conditions: This issue occurs after performing SSO.

  Workaround: There is no workaround.

- CSCue91533

  Symptom: Traffic through VPLS pseudowire is flooded due to MAC aging.

  Conditions: This symptom is observed when bridge descriptor index (internal index) assigned to MAC address exceeds 20480.

  Workaround: There is no workaround.

- CSCue93989

  Symptom: Less traffic received then expected rate for IMA link.

  Conditions: This issue occurs when IMA group is configured with 16 OC-3 T1 links. 888 pvcs are created and traffic is sent to only one pvc.

  Workaround: There is no workaround.

- CSCue94811

  Symptom: Process crash on standby does not generate a core file.

  Conditions: This issue occurs on normal conditions.

  Workaround: There is no workaround.

- CSCuf02518

  Symptom: IPv4 Traffic gets affected on IPv6 ACL applied interface.

Condition: This issue occurs if IPv4 ACLs and IPv6 ACLs in the system share the same label. The IPv4 traffic on the interface on which IPv6 ACL is applied is impacted.

Workaround: There is no workaround.

- CSCuf05039

  Symptom: I2C_WRITE and MDIO_READ/WRITE error messages are seen on the router.

  Conditions: This issue occurs on IM hard or soft OIR.

  Workaround: There is no workaround.

- CSCuf07508

  Symptom: The Gigabit Ethernet port on IMA8S may not come up after reload at times.

  Conditions: This issue occurs when the router is reloaded multiple times.

  Workaround: Perform an IM OIR.

- CSCuf42166

  Symptom: BERT Errors and Path Code Violations counter keeps incrementing.

  Conditions: This issue occurs when connected to E1E1 IM or the second PHY.

  Workaround: Connect to first PHY.

- CSCuf43275

  Symptom: The router does not detect or support traffic through GLC-FE-100EX and GLC-FE-100ZX transceivers.

  Conditions: This issue occurs under normal conditions.

  Workaround: There is no workaround.

- CSCuf48156

  Symptom: Local fault is seen on a 10 Gigabit Ethernet port.

  Conditions: This issue occurs when the interface is not shut and fibre is not connected.

  Workaround: Shutdown the interface

- CSCuf51429

  Symptom: Fast-Reroute FMFP-3-OBJ_DWNLD_TO_CPP_FAILED message seen on the console.

  Conditions: This issue occurs on shutting the link between the routers.

  Workaround: There is no workaround.

- CSCuf51462

  Symptom: Remote maintenance end points (MEP)s do not learn Port MEP on PC member links.

  Conditions: This issue occurs when port MEPs in PC member links are configured and remote MEPs do not learn it.

  Workaround: Configure Ethernet Virtual Connections (EVC) bridge domain and MEP PC member links.

- CSCuf51509

  Symptom: WRED counters for CS0 do not display in **show policy-map interface** command.

  Conditions: This issue is observed when **show policy-map interface** command is executed.

  Workaround: There is no workaround.

- CSCuf61365

Symptom: VC Counters do not increment On IM OIR followed by SSO.

Conditions: This is seen on HA system when IM OIR is followed by SSO switchover is performed.

Workaround: There is no workaround.

- CSCuf64704

  Symptom: "%MPLS-3-OUT_OF_LABEL3_SPACE: SIP0: nile_mgr: Out of resource to create" labels errors are seen on the console.

  Conditions: This issue is seen with scaled configurations, when LDP peer goes down and recovers.

  Workaround: Reduce the scale.

- CSCuf65040

  Symptom: The 1G or 10G IM may go in out of service state after a hard OIR of the IM.

  Conditions: This issue occurs after a hard OIR is performed.

  Workaround: Perform a another hard OIR or a SSO switchover followed by a soft OIR.

- CSCuf66022

  Symptom: The 10 Gigabit Ethernet interface status goes down on one side.

  Conditions: This issue occurs after shutting down the Ten Gigabit Ethernet interface and SSO is performed.

  Workaround: Perform a **shutdown** followed by a **no shutdown** 10 Gigabit Ethernet interface

- CSCuf74072

  Symptom: Seeing CRC errors on SFP IM with CU SFP.

  Conditions: This issue occurs when the CU SFP is configured with 100Mbps speed.

  Workaround: There is no workaround.

- CSCuf83316

  Symptom: Traffic loss of more than 1sec was observed during router reload.

  Conditions: This issue occurs on issuing **reload** command in middle router with R-LFA in RING topology.

  Workaround: There is no workaround.

- CSCuf83453

  Symptom: The **show ethernet service instance stats** command displays "0" at Egress stats counters.

  Conditions: This issue is seen after using **show platform hardware pp active asic stats** command.

  Workaround: Reload the router.

- CSCuf83886

  Symptom: Label exhaust message is seen even on valid case if policy is configured before xconnect is configured on scaled configuration.

  Conditions: This issue occurs when a service-policy is configured before configuring xconnect on the router that has consumed close to max labels.

  Workaround: First configure xconnect and then configure service-policy

- CSCuf93174

  Symptom: Packet Over SONET (POS) interfaces counters do not display correctly.

  Conditions: This issue occurs after SSO is performed. The issue is observed on the standby router.

  Workaround: There is no workaround.

- CSCug05647

  Symptom: Interface counters not getting updated with IP traffic.

  Conditions: This issue occurs when pinging back to back connected interfaces; the interface counters stay at 0.

  Workaround: Reload the device.

- CSCug07795

  Symptom: NQATM errors seen while adding new entries to ACL control region.

  Conditions: This issue occurs on bootup. The last 2 ACL control entries fail to get programmed.

  Workaround: There is no workaround.

- CSCug10134

  Symptom: Traffic is not flooded on port-channel by default, as IGMP does not support port-channel traffic.

  Conditions: This issue occurs when the incoming port is a Layer3 and outgoing is port is a BDI.

  Workaround: There is no workaround.

- CSCug16244

  Symptom: Traffic will not flow through few EoMPLS VCs.

  Conditions: This issue is seen with scaled EoMPLS configurations.

  Workaround: There is no workaround.

- CSCug22122

  Symptom: IOMD crash is seen for any IM on the router.

  Conditions: The IOMD crash is seen when **show platform software agent iomd 0/1 driver stats** command is executed to verify driver statistics.

  Workaround: There is no workaround.

- CSCug23372

  Symptom: Manager process crash occurs while configuration replace operation is performed.

  Conditions: This issue occurs while moving from REP to G8032.

  Workaround: Avoid performing a configuration replace.

- CSCug26991

  Symptom: OSPF session goes down after applying the policy on EC main interface, EC EVC and EC Trunk EFP.

  Conditions: This issue occurs after applying the policy EC main interface which has OSPF session enabled. The OSPF session goes down after application of Egress policy.

  Workaround: Apply policy directly on EC member links.

- CSCug40852

  Symptom: Link failure in L3VPN core takes a long time to converge with BGP PIC configuration.

Conditions: This issue occurs when BGP PIC core and PIC edge is configured and there are more than one ECMP core paths to reach backup BGP peer.

Workaround: Configure only one core path to reach both primary and repair BGP Peers in a BGP PIC Core and Edge configuration. If there are more than one equal cost physical paths to reach BGP peers, then adjust the configuration by increasing the distance for all paths except one.

- CSCug44908

  Symptom: Traffic goes down after applying policy-map without ingress classification.

  Conditions: This issue occurs when without classifying the traffic in the Ingress, this policy map is applied in the egress port.

  Workaround: Edit the policy map by changing the bandwidth percentage number.

- CSCug45557

  Symptom: Ingress marking does not work when Egress marking has a match on qos-group.

  Conditions: This issue occurs when ingress marking is not working when Egress marking matches on qos-group.

  Workaround: There is no workaround.

- CSCug45618

  Symptom: OSPF does not come up with policy map having 2 different EFP classes and configured on 2 different interfaces.

  Conditions: This issue is observed only when same policy map is applied on 2 interfaces with one EFP in the policy map.

  Workaround: Remove the policy map from one of the interfaces to bring up the OSPF.

- CSCug46010

  Symptom: The non IP packets get classified under the second class instead of class-default when two class-maps one having match on L4 ACL and other having match on L3 ACL with permit ip any any is configured.

  Conditions: This issue occurs when two class-maps one matching on L3 ACL match and another matching on TCP or UDP are configured.

  Workaround: There is no workaround.

- CSCug46157

  Symptom: When an existing policer is deleted and added back, the policer fails to take effect.

  Conditions: This issue occurs when the policing was dynamically deleted and added.

  Workaround: Remove the policy-map and re-apply on the interface or EFP.

- CSCug57503

  Symptom: ESP crash observed on the router.

  Conditions: This issue occurs after executing the **show platform hardware qfp** command on the active feature packet-trace configuration.

  Workaround: Do not execute unsupported command.

- CSCug61357

  Symptom: The ISIS router fails to come up after issuing a **shutdown** followed by a **no shutdown** command.

  Conditions: This issue occurs when RLFA and BFD configutations exist on the router.

Workaround: Issue a **shutdown** followed by a **no shutdown** command again.

- CSCug61508

  Symptom: Classification based on ACL in the child does not work

  Conditions: This issue occurs when the parent classification is EFP.

  Workaround: There is no workaround.

- CSCuf65301

  Symptom: Micro flaps observed on the router.

  Conditions: This issue is seen when system is kept idle for hours.

  Workaround: There is no workaround.

- CSCug67955

  Symptom: The standby FP is stuck in init state.

  Conditions: This issue occurs after ISSU is performed.

  Workaround: There is no workaround.

- CSCug71853

  Symptom: BFD flaps are observed on the router.

  Conditions: This issue is seen when traffic flows at line rate.

  Workaround: Keep traffic at around 90% line rate.

- CSCug72785

  Symptom: OSPF flap observed on the router.

  Conditions: This issue occurs after IM OIR followed by SSO.

  Workaround: There is no workaround.

- CSCug73776

  Symptom: The standby router crashes on bootup when highly scaled configurations and when L2VPN and multicast are configured.

  Conditions: This issue occurs on reloading the router 3-4 times with highly scaled configurations and L2VPN and multicast are configured.

  Workaround: There is no workaround.

- CSCuh18073

  Symptom: In a domain with 2 BGP exit points acting in Active or Repair mode, traffic would be exiting the domain through Repair path BGP PE instead of exiting through Active path BGP PE.

  Conditions: This issue occurs in the following conditions:

  - Environment has 2 BGP exit points
  - A change in one of the core links to the primary BGP exit point results in Repair BGP PE becoming Active BGP PE and vice versa

  In this scenario, even after BGP convergence, data packets would traverse through previous primary BGP PE(now repair path PE).

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.9(0)S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 Router in Cisco IOS XE Release 3.9(0)S.

- CSCud06772

  Symptom: IPv6 neighbor discovery does not function properly after stateful switchover (SSO); the router loses traffic and eventually recovers.

  Conditions: Occurs with IPv6 traffic after stateful switchover (SSO).

  Workaround: Configure software BFD sessions.

- CSCud29491

  Symptoms: Simultaneous policy can be applied

  Conditions: On physical interface (having efps) and on efps (on that physical interface)

  Workaround: None. As it is an unsupported config.

- CSCud35732

  Symptoms: The router does not apply egress CFM MIP filtering.

  Conditions: Occurs when you overwrite a MIP configuration using the **ethernet cfm mip level** command.

  Workaround: Instead of overwriting the MIP level configuration, remove and re-apply the configuration.

- CSCue34781

  Symptoms: The policer in the parent policy-map of an hqos policy attached to an interface stops working after the child policy policer is dynamically modified.

  Conditions: Occurs when the policy-map attached to the interface is a hierarchical policing policy and both the child and parent policy-map have policing actions in their classes. The policing in the parent class does not work correctly after you dynamically modify the policing action in the child policy.

  Workaround: Remove and re-attach the policy-map on the interface

- CSCue41416

  Symptoms: IOMD CPUHOG messages seen on ASR903

  Conditions: Seen when ISSU upgrade is performed between two XE39 images

  Workaround: None

- CSCue42139

  Symptoms: The ptp state is stuck in acquiring state all the time.

  Conditions: When pulled out the active RSP, the T3 time-stamping is stuck and the ptp state stays in acquiring state all the time.

  Workaround: Reload the IM or unconfigure or configure the ptp.

- CSCue46274

  Symptoms:

  Traffic flow stops over a particular prefix configured on TDM interface and Crash while executing show platform prefix command for the same prefix

  Conditions: Configure route via a TDM interface and reload the router once.

Workaround: No workaround

Further Problem Description: With only Gigabit Ethernet interfaces this problem is not seen. Only when we have TDM interface we see the problem**.**

- CSCue63229

  Symptoms: IMA interfaces flap frequently every 15–30 minutes. The issue does not occur on member links.

  Conditions: Occurs when you increase the number of member links in the IMA group to 16.

  Workaround: There is no workaround.

- CSCue65149

  Symptoms: When changing the interval in evc bd offload cases(scale) getting OBJ messages.

  Conditions: First configure the 3.3ms interval and meps after that removed the meps,domain and configure 10ms interval and meps will hit this issue.

  Workaround: Configure very less session

- CSCue66019

  Symptoms: output errors will be seen on mlppp interfaces.

  Conditions: With 90% and above Line rate traffic with mix MTU patterns (IMIX), output errors will be seen on the mlppp interface.

  Workaround: No. The issue is seen for IMIX pattern traffic with 90% & above Line rate traffic.

- CSCue67245

  Symptoms: MFIB counters for some of the (S,G) are not updated on ASR903

  Conditions: Is seen when we scale the number of Sources. Issue is seen for 2000 sources joining 1 group. No impact to traffic

  Workaround: There is no workaround.

- CSCue67267

  Symptoms: High Traffic drop seen on SSO Double dip seen on SSO

  Conditions: Issue is seen occassionally (one in 5 iterations) on ASR903 with MVPN scale setup.

  Workaround: There is no workaround.

- CSCue67995

  Symptoms: Nile manager crashes while flapping mpls enabled interface on the peer end nodes.

  Conditions: 6K routes L3VPN routes and 600 L2VPN sessions with flaps can crash nile manager of ASR903 at uea_untyped_dqueue_remove_elem

  Workaround: No workaround

- CSCue70575

  Symptoms: Kernel crash is observed

  Conditions: On reload kernel crash is seen

  Workaround: There is no workaround.

- CSCue72481

  Symptoms: IP address and Meps accepting in the same interface

  Conditions: configured the IP address and Port mep accepting in the same interface.

Workaround: There is no workaround.

- CSCue75775

  Symptoms: fman fp crash causes router to crash with scale of 16000 queues on rsp1b

  Conditions: large scale qos configurations

  Workaround: There is no workaround.

- CSCue76109

  Symptoms: DMM reports delay of 0ns.

  Conditions: Have Y1731 DMM sessions with CFMoXconnect and MPLS TE tunnels in the core.

  Workaround: No Workaround. Having a single path between the 2 MEPs can avoid this.

- CSCue77596

  Symptoms: cos vlaue gets wrongly marked for a qinq packet

  Conditions: a service instance with dot1q encap and no rewrite is configured on the interface... the policy map attached in the ingress has marking in it... the packet should not be ,marked in this case... but on asr903 its getting marked wrongly

  Workaround: There is no workaround.

- CSCue86047

  Symptoms: Pkts Not Classified On Removing/Re-applying Marking action dynamically

  Conditions: A class-default policy with marking action is applied and nn removing/re-applying exp marking action of the class-default, packets are not hitting the class-default and policy-map counters do not increment. This issue is seen on any type of interface.

  Workaround: Instead of removing & adding marking action alone, detach the policy itself from the interface, modify the marking action and re-attach the policy to the interface.

- CSCue87175

  Symptoms: BFD sessions may flap on an ASR903 router.

  Conditions: With around 2000 global IPv4 prefixes and with traffic running, when a core-facing interface is shutdown on a router in the ring, BFD flaps may be seen on another router in the ring.

  Workaround: There is no work-around known as yet.

- CSCue87629

  Symptoms: INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client 'iosd-nile' messages may appear on the console. **Conditions:** When a shut/no shut of G8032 ring interface of Peer or local device is done.

  Workaround: No workaround.

- CSCue90720

  Symptoms: IPCP state mismatch and member link state mismatch in ppp multlilink on back to back to connection. Traffic will get dropped

  Conditions: Bundle having maximum links in it and perform a SSO. find steps to repro

  Workaround: none

- CSCue96512

  Symptoms: RP crashes if punt/inject keepalives are missed.

Conditions: Punt/inject keepalives are missed and we are not holding a TTY while writing to punt/inject log file.

Workaround: none

- CSCue96886

  Symptoms: Complete MAC Address space is not available on the RSP

  Conditions: Removing the Service instance with the MAC Addresses learnt on the BD.

  Workaround: Reload the Router is only workaround.

- CSCue97114

  Symptoms: Shut down the trunk efp in core side, meps are learnt for UP MEP

  Conditions: Configured UP Mep evc bd (core side trunk efp) when i shut the trunk efp in core remote meps are learnt for UP MEP.

  Workaround: Configure evc bd in core side

- CSCuf05090

  Symptoms: Standby will be resetting continuously with running config sync failure.

  Conditions:

  Downgrade all IMs and take the IMS out of slot.After booting up with XE39 image , insert IMs one by one. While upgrade was happening , this issue happened.Im got crashed and stanby was resetting continuously with SYNc failed.

  Workaround: Reload the box completely.

- CSCuf20275

  Symptoms: On interoperating with an ASR901 router, BFD sessions may flap as the ASR903 router may some times not send BFD control messages.

  Conditions: With around 200 global IPv4 prefixes, BFD session running in software with echo OFF and seen even without any data traffic.

  Workaround: There is no work-around known as yet.

- CSCuf44077

  Symptoms: show interface output is showing wrong speed values after sso

  Conditions: when we use the 100M SFP’s

  Workaround: There is no functionality impact because of this. HW module reset will resolve this.

- CSCuf56723

  Symptoms: Interface LED glows green with shut.

  Conditions: After SSO

  Workaround: No workaround.

- CSCuf60346

  Symptoms: IOMd Crash On Performing SSO Switchover With Interfaces Shut

  Conditions: Have ATM/IMA interfaces shut. Perform switchover and notice IOMd crash on new Active

  Workaround: No workaround

- CSCuf64404

Symptoms: IOMD crash will be seen when flap is performed on remote router. The flap can be by shut/no shut or IM oir.

Conditions: IOMD crash seen on multiple mlp bundle flap becoz of memory leaks in wintegra.

Workaround: None.

- CSCuf64625

  Symptoms: CRC Errors reported on RevD IM

  Conditions: IM OIR or SSO

  Workaround: No workaround.

- CSCuf64695

  Symptoms: Error message seen on PE ASR903 :- *Mar 22 11:51:35.929 IST: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: SIP1: fman_fp_image: atom_xconnect xid 0x1004013, ifh 16793619, dirty 0x1, state 0x2 download to CPP failed

  Conditions: CEM configs on OC3IM and/or T1E1IM. Reported with CESOP circuits and scale of about 88. Seen with less scale also. Seems to be a non-function impacting message.

  Workaround: None.

- CSCuf64811

  Symptoms: Serial Links on CEs are in up/down state, when configured with CEM CeSop circuits on PEs.

  Conditions: Configure CEM cesop circuits over MPLS core. Note that the serial interfaces on CE routers are UP/UP. Perform a SSO on PE2 router.

  Workaround: Perform another SSO on PE2 router and issue is solved.

- CSCuf65012

  Symptoms: Seeing syslog for the port 0/5/0 saying it is down which is used for HFPGA

  Conditions: IM oir of Slot 4 or Slot 5

  Workaround: No Functionality impact and no workaround.

- CSCuf74072

  Symptoms: Seeing CRC errors on SFP IM with CU SFP.

  Conditions: When the CU SFP is configured with 100Mbps speed.

  Workaround: No workaround.

Resolved Caveats—Cisco IOS XE Release 3.9(0)S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.9(0)S.

- CSCts14725

  Symptoms: mep does not come up sometimes, error messages always.

  Conditions: change cc interval on the fly.

  Workaround: None.

- CSCts95896

  Symptoms: The router stops passing traffic on EVC interfaces.

Conditions: Occurs when you issue the default interface command and immediately restore the configuration. The issue occurs with configurations containing either a large number of EFPs or features that impact EFP programming at a lesser scale, such as QoS.

Workaround: Wait for the router to clear the old EFP configuration before adding a new configuration.

- CSCtu39377

  Symptoms: "sh running" , "sh romvar" in exec mode and "set" command in rommon mode, displays multiple entries for the license being used.

  Conditions: ASr903 with appropriate license and boot level set.

  Workaround: No workaround.

- CSCtx44513

  Symptoms: The router stops passing traffic on an interface

  Conditions: Occurs when you remove all classes from a QoS policy-map attached to an interface.

  Workaround: Remove and re-attach the policy-map.

- CSCtx44688

  Symptoms: Cannot configure policing and marking together in the same class of the egress policy-map.

  Conditions: Set and police statements together in the same class of a policy is rejected at the CLI.

  Workaround: In order to achieve marking and policing at the ingress we can use a conditional policer but this is not supported at the egress.

- CSCtx70302

  Symptoms: Traceback and Log message seen on performing a multilink bundle shut on ASR903 as described in the summary.

  Conditions: Traffic should be flowing over the multilink bundle. Multiple ways to trigger the same issue, but traffic and mlppp bundle remain common to each scenario.

  Workaround: None. Harmless traceback.

- CSCty73682

  Symptoms: A small percentage of IPv6 packets that should be blocked by an interface ACL is instead pass through

  Conditions: In certain conditions, when an IPv6 ACL is applied to an interface, a small percentage of IPv6 packets that would otherwise be dropped, will instead bypass an ACL and get through.

  Workaround: None

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:U/RC:C CVE ID CVE-2012-3946 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz20839

  Symptoms: IMA functionality does not work properly.

  Conditions: Occurs after an RSP switchover when the router is running an IMA configuration.

Workaround: Reload the interface module with the IMA configuration.

- CSCtz43467

  Symptoms: Not All CLI's listed under the REP configuration modes are allowed. For e.g The following configurations are allowed but will not work. 1) REP does not work on BDI. 2) More than 1 source ports in a span session.

  Conditions: Seen all the time.

  Workaround: No workaround

- CSCtz65778

  Symptom: The control plane goes down with VPNv6 traffic.

  Conditions: Occurs with 64-byte VPNv6 traffic. The issue only occurs for small, tunnelled packets.

  Workaround: There is no workaround.

- CSCtz87775

  Symptoms: An interface on the OC-3 interface module does not become active.

  Conditions: Occurs when you change the interface mapping between au-4 and au-3 when changing an interface between T1 and E1 operation.

  Workaround: Perform a soft OIR on the interface module.

- CSCua16492

  Symptoms: Some IPv6 multi-hop BFD over BGP sessions flap.

  Conditions: Occurs on port-channel interfaces running IPv6 multi-hop BFD over BGP sessions after you perform an SSO.

  Workaround: There is no workaround.

- CSCua35446

  Symptoms: gig 0/5/0 interface displayed in PRIME software.

  Conditions: System being up.

  Workaround: No workaround.

- CSCua37816

  Symptoms: "DHCP_SNOOP: Failed sending packet out of BD" errors on standby.

  Conditions: DHCP snooping enabled with asr903 as relay with HA system.

  Workaround: No workaround. Wont be seen on standalone system.

- CSCua46443

  Symptoms: Y1731 frames were received and forwarded by STP blocked port and hence database is corrupted.

  Conditions: When 2 or more interfaces are there b/n the devices and only one is forwarding and remaining blocked by STP.

  Workaround: None.

- CSCua49623

  Symptoms: CEM interface becomes inaccessible

  Conditions: When same channel-group number and cem-group number is used for overlapping timeslots this issue is hit

Workaround: Use different timeslots, or make sure channel-group and cem-group numbers are different under the same controller

- CSCua57325

  Symptom: The router displays an OIR SPA error.

  Conditions: Occurs under the following conditions:

  - The router is running offloaded CFM sessions over an xconnect (pseudowire) interface.
  - The router is using a redundant hardware (dual RSP) configuration.
  - The remote router is using a non-redundant (single RSP) hardware configuration.
  - You reload the router.
  - **Workaround:** There is no workaround.

- CSCua61934

  Symptoms: When policy-map with priority in class-default is attached to interface its not getting rejected.

  Conditions: Configure policy-map having priority in class-default. Attach the policy to interface it's not getting rejected.

  - **Workaround:** None known at this time

- CSCua77688

  Symptom: The router experiences remote CFM MEP flapping.

  Conditions: Occurs when the router is connected via a CFM xconnect and the link is running a high traffic rate.

  Workaround: Reduce the rate of traffic.

- CSCua90879

  Symptom: QoS policies with a police statement on the class-default class do not take effect.

  Conditions: Occurs when you apply a police statement to the class-default class within a QoS policy on an ingress EVC interface.

  Workaround: Apply the police statement to a static class, such as class cos0.

- CSCub18160

  Symptom: The router drops traffic on a link twice and displays a remote fault error message.

  Conditions: Occurs when you issue an interface module reset (OIR) while the 10.000M XFP (DWDM Edge performance) or XFP10GER-192IR-L XFPs are plugged into the ten Gigabit Ethernet interface module and active.

  Reloading the router also takes significantly longer when using these XFPs.

  Workaround: There is no workaround.

- CSCub26877

  Symptoms: When Bridge-domain of the efp is changed and the new bridge-domain is not accepted, the old bridge-domain gets rejected.

  Conditions: EVC -BD configuration change.

  Workaround: None

- CSCub33576

  Symptoms: All IMA interfaces does not come up until OIR of IM.

Conditions: When IMA are configured.

Workaround: OIR.

- CSCub33664

  Symptoms: High Delay values seen when using DMM Sesssion on ASR903 post SSO.

  Conditions: Delay values will be higher only after SSO on ASR903.

  Workaround: Remove and reconfigure DMM sessions again post SSO on AR903.

- CSCub38619

  Symptoms: System crashes when COS value for vlan under an EFP is modified.

  Conditions: This happens only when a prior operator attempt to modify the COS value failed. This failure can be due to incompatible efp match conditions on the egress efp.

  Workaround: None

- CSCub41772

  Symptom: Router console is flooded with CPUHOG and EVENTLIB messages.

  Conditions: The issue occurs rarely when you issue multiple interface module reset (OIRs), RSP switchovers (SSO), or reloads while using a configuration with a high number of T1 serial links on the OC-3 interface module.

  Workaround: There is no workaround; however, the messages to not affect router functionality.

- CSCub48129

  Symptoms: CFM CCM's were being sent out on egress interface with cfm disabled.

  Conditions: Configure UP mep on EVC BD.DIsable cfm on the egress interface.

  Workaround: There is no workaround.

- CSCub49985

  Symptoms: MPLS pseudowire ping from the peer to the Cisco ASR 903 fails if the peer is using TTL-based ping.

  Conditions: This symptom occurs when the peer is using TTL-based ping.

  Workaround: There is no workaround.

- CSCub50110

  Symptoms: Tx timer table not programmed after shut/no shut for hardware offload BFD. It is not consistently seen.

  Conditions: The issue is seen while we do shut/no shut on BDI/Physical interface which has BFD configured.

  Workaround: None.

- CSCub50487

  Symptoms: The router accepts a rewrite push statement on an EFP configured with QinQ encapsulation.

  Conditions: Occurs when you configure an xconnect EFP with QinQ encapsulation and a rewrite push statement.

  Workaround: There is no workaround.

- CSCub52571

  Symptoms: Traceback seen on console. This traceback doesn't impact any functionality

Conditions: Traceback seen when BFD is enabled and flapped the interface where IPv6 BGP/OSPFv3/BFD is already UP.

Workaround: No Workaround. This ddts fixes the traceback occurrence.

- CSCub52657

  Symptoms: CPP object download failure messages are seen while creating BDI interface.

  Conditions: The problem is seen when the user tries to configure the BDI interfaces exceeding the platform limit. On asr903 RSP1A and RSP1B the maximum BDI interface limit is 256 and 1024 respectively. When user tries to exceed this limit the error message is seen as download failure on the console, this is not a bug.

  Workaround: Not to exceed the BDI interface limit set for the platform

- CSCub55760

  Symptom: The router displays a Delay Measurement Message (DMM) delay value of 0.

  Conditions: Occurs under the following conditions:

  - You configure an EVC down MEP on a port-channel interface.
  - You dynamically add a member link to a port-channel interface.

  Workaround: Configure PTP synchronization before scheduling DMM.

- CSCub59776

  Symptoms: Router seems hang post removal of startup-config and reload

  Conditions: Router has no startup config present.

  Workaround: The following dialogue was missing to appear on the console.

  --- System Configuration Dialog ---

  Would you like to enter the initial configuration dialog? [yes/no]: % Please answer 'yes' or 'no'.

  Just type no, and start the configuration dialogue later.

- CSCub60668

  Symptom: The router is unable to establish an OSPF session.

  Conditions: Occurs when you enable an OSPF session over an MPLS TP tunnel.

  Workaround: There is no workaround.

- CSCub63072

  Symptom: MPLS convergence can be slower than expected.

  Conditions: Occurs when the router switches to a backup MPLS path in the event of a network failure.

  Workaround: You can configure the following redundancy features to protect against network failures:

  - IPv4 Loop Free Alternate Fast Reroute (LFA FRR)
  - Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC)
  - MPLS Traffic Engineering (TE)--Fast Reroute (FRR) Link and Node Protection

- CSCub63954

  Symptoms: Speed configurations are rejected. Error message appears on active

  Conditions: HA - Box. Speed configurations are rejected

Workaround: No Workaround.

- CSCub71578

  Symptoms: The router displays traceback and failure messages on the standby RSP.

  Conditions: Occurs after you issue an OIR on the T1/E1 interface module from the active RSP. The issue occurs in a redundant system.

  Workaround: There is no workaround.

- CSCub74338

  Symptoms: The router crashes.

  Conditions: Occurs when you attach an ingress QoS policy-map to an EVC with a rewrite push configuration.

  Workaround: There is no workaround.

- CSCub76908

  Symptoms: If Y1731(DMM or SLM) sessions are configured for UP MEP, where the core facing and access interfaces have different encaps, then Y1731 sessions will not come up

  Conditions: The condition will be same if the encaps are same and if rewrite ingress pop is configured

  Workaround: None

- CSCub80685

  Symptoms: On BDI Shut, if routing traffic continues, it will be punted to the CPU which will flood out the CPU resulting in control plane loss

  Conditions: Ping failure and BFD/OSPF flaps on BDI shut while ipv4/v6 traffic is running while BDI is shut.

  Similar conditions occur on no EFP/BDI configured or no ip address configured.

  Workaround: Stop routing traffic into shut BDI port.

- CSCub84828

  Symptoms: Iosd crash on standby when booting up

  Conditions: Boot up of standby

  Workaround: RSP has to be booted again.

- CSCub85398

  Symptoms: On customer's setup the following error message is seen. Dec 2 15:41:40.970 JST: %NILE_ASIC-2-TCAM_PARITY_ARRAY_ERR: TCAM4 Parity Array Error at Asic: 1 TCAM Index: 0x306D Application: UCASTV4 Region UCAST_32.

  Conditions: No specific condition. There are no any operation or network events at that time.

  Workaround: On reloading the box the message is disappeared.

- CSCub88805

  Symptoms: When alarms are seen it displays as ASR1000 instead of ASR903, no functionality impact, only display issue.

  Conditions: On seeing alarms.

  Workaround: None.

- CSCub88822

Symptoms: NULL_DATA_STRUCTURE traceback is seen on ASR903 console.

Conditions: Issue is seen when OC3IM is present on the box and IM OIR is done on this OC3IM. Usually seen when no configs are present on IM. Quite inconsistent, not always seen.

Workaround: None. The traceback does not affect any functionality.

- CSCuc00853

  Symptoms: ARP requests are not flooded on bridge-domains

  Conditions: Dynamic ARP inspection configured on bridge-domains

  Workaround: None

- CSCuc07697

  Symptoms: BIT-4-OUTOFRANGE: tracebacks flooded on the console.

  Conditions: Configure CFMoTEFP and vlan load-balancing for the BDs part of REP segment. Tracebacks are seen only when there is an untagged efp on the interface and there is an AIS condition.

  Workaround: Do not have BD with untagged EFP on the box.

- CSCuc07747

  Symptoms: On entering "show debugging" command on ios prompt, the following extraneous messages are seen,

  % Invalid input detected at ’^’ marker.

  Conditions: Seen in all conditions.

  Workaround: No workaround. Though this doesn’t have any functionality impact. Only issue is the extra prints.

- CSCuc07759

  Symptoms: ARP responses are dropped

  Conditions: Dynamic arp inspection is configured on the router

  Workaround: None

- CSCuc08098

  Symptoms: Trap config for AAA-SERVER mib is missing.

  Conditions: When a asr903 device is loaded with metroaggrservices license.

  Workaround: None.

- CSCuc12681

  Symptoms: Intermittent packet drops when doing MPLS ping

  Conditions: MPLS ping Rate has to exceed 1Mbps. sweep ping with high range High number of frames with huge pkt size

  This is not applicable to IP icmp ping. Only applicable for MPLS ping.

  Workaround: Try a lower number of frames.

- CSCuc21610

  Symptoms: The console displays a message indicating that offloading is not supported for BFD echo mode.

  Conditions: Occurs when you configure a BFD session in echo mode.

  Workaround: There is no workaround; however, the issue has no functionality impact.

- CSCuc25058

  Symptoms: Forced QL value on BITS port gets overwritten when a new primary clock source with different QL value is selected.

  Conditions:

  Network clocking should be enabled in QL mode and with BITS port configured to output system clock with forced QL value.

  Workaround: Reconfigured the forced Tx QL value on the BITS port after the system switches to clock source with different QL value than the current selected.

  Further Problem Description: When the system selects a new primary clock source, it propagates the QL value of that primary clock source on all the timing ports, so that all timing ports reflect the system QL value. When this update is send the forced TX QL value configured on each port gets overwritten by the system QL Value.

- CSCuc34088

  Symptom: The router passes lower traffic levels when you add links to an IMA bundle and perform IM OIR/router reload.

  Conditions: Occurs when you send traffic above the E1 line rate on one link within an IMA bundle and reset (OIR) the interface module.

  Workaround: Remove and re-apply the IMA interface configuration.

  CSCuc35618

  Symptoms: REP session flaps post SSO and traffic is dropped until the session re-converges after the SSO.

  Conditions: Upon SSO.

  Workaround: None

- CSCuc36241

  Symptoms: The router is unable to select a given PTP clock as a network clock source.

  Conditions: Occurs when you configure PTP as an input network clock source while the slave clock is still in a holdover state. In the holdover state, the slave clock has not yet attempted to establish a frequency lock with a master clock.

  Workaround: Wait for the PTP slave clock to lock to the master clock before configuring PTP as a network clock input source.

- CSCuc36381

  Symptoms: CLI show satellite env and show satellite alarm not displaying any output.

  Conditions: Show satellite env and show satellite alarm CLI is not supported in satellite mode in 4.3.0

  Workaround: Can check the status in ASR9k.

- CSCuc41871

  Symptoms: ATM interfaces stay down during normal operations

  Conditions: 1. Post router reload 2. When peer interface cable is pulled out & put back

  Workaround: Interface reset (shut/no shut)

- CSCuc42002

  Symptoms: The router crashes when configuring the ATM interface, displaying a segmentation fault error.

Conditions: This symptom is observed when you move an OC-3 interface module with an ATM configuration to a different bay and configure an ATM interface on the new bay.

Workaround: There is no workaround.

- CSCuc42117

  Symptoms: The router does not include 0xff03 flag leading bits within ppp fragment messages.

  Conditions: Occurs when the router has not negotiated ACFC.

  Workaround: There is no workaround. Most remote devices should ignore this behavior by design, but some devices may display unexpected behavior, such as for IPCP PROTREJ messages.

- CSCuc43719

  Symptoms: ASR903 with dual RSP may crash.

  Conditions: No specific trigger, but any configuration related to NBAR can make the box hit this issue.

  Workaround: Do not have any NBAR configurations on the box as these are not supported on ASR903.

- CSCuc57130

  Symptom: The router does not apply OC-3 interface module (IM) configurations.

  Conditions: Occurs after an RSP switchover.

  Workaround: There is no workaround.

- CSCuc59386

  Symptoms: Continuous iomd crash on oc3im. Interfaces on oc3im not configurable, error message seen :- stand-by dosen't support this command

  Conditions: Seen on a HA ASR903 setup with oc3im. Seen when a iomd crash happens on active rsp and then standby iomd session handle is not cleared.

  Workaround: Reload the stand-by rsp.

- CSCuc60148

  Symptoms: System is not shutting down upon temperature sensor reaching 'SHUTDOWN' threshold region.

  Conditions: Temperature sensors reached shutdown threshold region

  Workaround: IOS config command has to be explicitly configured to enable this system shutdown behavior. 'facility-alarm critical exceed-action shutdown'

- CSCuc62784

  Symptoms: Traces @ niles_if_count_initialize some times

  Conditions: On performing Reload, Standby Reload, SSO

  Workaround: No workaround. And these traces are displayed on the console and does not have any functionality impact to the system.

- CSCuc64509

  Symptom: ASR903 as PTP master transmits clock class corresponding to holdover state on fresh bootup.

  Conditions: ASR903 is not connected to any external frequency and Phase source and is using freerun internal clock to provide synchronization.

  Workaround: ASR903 PTP master should be locked to external frequency and phase source.

Further Problem Description: ASR903 when locked to internal free-running clock, then ASR903 PTP master function transmits clockclass value 14 which corresponds to holdover state instead of 58 which corresponds to free-running clock.

- CSCuc64899

  Symptom: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: Occurs on interfaces with an xconnect statement after a reload on a peer device.

  Workaround: Remove and re-apply the CFM configuration.

- CSCuc66393

  Symptom: The router loses OC-3 interface configurations after an ISSU upgrade.

  Conditions: Occurs on OC-3 serial and POS interfaces after an ISSU software upgrade.

  Workaround: There is no workaround.

- CSCuc66895

  Symptom: Layer 2 traffic loop seen in REP topology for a transient time, when the Cisco ASR 903 which is a part of the REP ring is reloaded.

  Conditions: This symptom is observed when the Cisco ASR 903 is part of an REP ring, and the box is reloaded with saved REP configurations.

  Workaround: Traffic loop is transient, once REP convergence looping is stopped.

- CSCuc68246

  Symptom: The standby IOMD crashes on booting up the standby RSP.

  Conditions: This symptom occurs when booting up the standby RSP with a configuration that is already present.

  Workaround: Boot up the standby without any configurations and start configuration once the standby has reached STANDBY_HOT state.

- CSCuc68462

  Symptom: The router drops PTP traffic.

  Conditions: The issue occurs occasionally when you configure PTP slave clock to receive VLAN-tagged traffic.

  Workaround: There is no workaround.

- CSCuc70509

  Symptom: Packet rate counters i.e. packets per second is not cleared to 0 when interface goes down.

  Conditions: Applies to all TDM interfaces like serial , mlppp , POS , etc. Issue seen on controller shut etc, not seen on interface shut.

  Workaround: None. Should be fixed now.

- CSCuc71410

  Symptoms: Config sync failure but it doesn't have much of an impact on the service

  Conditions: We have a mac limit configured with action as limit and when the configured limit is exceeded, the standby comes up after the limit is hit

  Workaround: none

- CSCuc71723

  Symptom: The router erroneously accepts a service-policy configuration on a CEM interface and displays it within the running configuration.

  Conditions: Occurs when you configure a service-policy on a CEM interface.

  Workaround: There is no workaround.

- CSCuc74205

  Symptoms: Tracebacks displayed continuously on performing IM OIR

  Conditions: Have CEM, ATM, IMA configured on a TDM IM. Now, on performing IM OIR, notice this traceback continuously on active RSP. This is noticed on performing OIR operation every 2 out of 5 times.

  Workaround: No workaround

- CSCuc81334

  Symptom: The router selects a clock source attached to standby RSP.

  Conditions: Occurs after a stateful switchover (SSO).

  Workaround: Remove and restore the clock source configuration.

- CSCuc81416

  Symptoms: Traces may be seen on active with SNMP configuration

  Conditions: Seen when Hard pull of Standby is done

  Workaround: Do soft reset/ sso switchover

- CSCuc83088

  Symptom: The router drops traffic during stateful switchover (SSO).

  Conditions: Occurs when the router is running HSRP or VRRP; the issue only occurs when the destination MAC address is a virtual MAC (vMAC) address.

  Workaround: Change the traffic priority and detour traffic prior to the SSO.

- CSCuc87791

  Symptom: The router selects a network clock source before the wait-to-restore timer has expired.

  Conditions: Occurs under the following conditions:

  – A clock source fails, triggering the wait-to-restore timer (which specifies how long the before including a restored clock source in the clock selection process.

  – The clock source becomes active and fails a second time before the wait-to-restore time has passed.

  Workaround: There is no workaround; in some cases you can clear the issue by removing and restoring the clock source configuration.

- CSCuc91582

  Symptom: Adding EFP to Bridge-Domain fails and errors are seen when reloading with Cisco IOS XE Release 3.7.1a.

  Conditions: This symptom is observed when reloading the Cisco ASR 903 with Cisco IOS XE Release 3.7.1a, when EFP and PW are in the same Bridge-Domain.

  Workaround: Post reload, remove the EFP configurations, and configure PW first and then EFP.

- CSCuc92953

  Symptom: The RSP crashes.

  Conditions: Occurs under the following conditions:

  - You configure Protocol-Independent Multicast-Sparse Mode (PIM-SM) with a static rendezvous point (RP).
  - You create an EVC port channel on the access side with one member link
  - You create bridge domain interfaces (BDIs) with 1:1 mapping between EVCs and bridge-domains.
  - You use the BDIs to send IGMP v2 static join messages to a single multicast group
  - On the remote device, you create 150 EFPs and map them to the BDIs.
  - You initiate multicast traffic.
  - You set the EFPs to the default configuration and add them to the existing port-channel

  The router crashes.

  Workaround: There is no workaround.

- CSCuc93985

  Symptom: The router initiates an Automatic Protection Switching (APS) switchover during a high availability (HA) stateful switchover (SSO).

  Conditions: Occurs during an HA SSO with single router APS (SR-APS).

  Workaround: There is no workaround.

- CSCuc95716

  Symptom: FPGA software for the OC-3 interface module is not bundled with the XE 3.8 image.

  Conditions: Occurs when upgrading FPGA on the OC-3 interface module.

  Workaround: Manually upgrade the OC-3 FPGA.

- CSCud01855

  Symptoms: APS switchover may occasionally lead to inconsistent/incorrect APS states with CEM config.

  Conditions: Seen when APS is configured with CEM/ATM on IM-4OS on ASR903. Caused due to notifications not being correctly sent to CEM subsystem.

  Workaround: No workaround.

- CSCud01908

  Symptom: Debug commands show pending objects on the Forwarding Manager (FMAN) on the forwarding processor (FP), indicating a failure to download configurations from the Route Switch Processor (RSP) to the data plane (DP).

  Conditions: Occurs when you apply a QoS shaping configuration at a high scale.

  Workaround: Delete the QoS policies and remove the QoS configuration from the interface.

- CSCud04407

  Symptom: The router displays the following console error message: `Error - packet with unsupported linktype 3`

  Conditions: Occurs when the router is passing traffic over the OC-3 interface module.

  Workaround: There is no workaround.

- CSCud07085

  Symptom: The serial interface on the OC-3 interface module remains in a down state.

  Conditions: Occurs when you migrate from T1 mode to E1 mode using the OC-3 interface module.

  Workaround: Issue an interface module reset (OIR) on the OC-3 interface module.

- CSCud07236

  Symptoms: Upon reload few harmless messages will seen.

  Conditions: Upon reload few harmless messages will seen.

  Workaround: No impact on device.

- CSCud07642

  Symptom: The ASR 903 is unable to pass traffic to the ASR 9000.

  Conditions: Occurs with a clear-channel ATM over MPLS configuration using AAL0 encapsulation.

  Workaround: Enable MPLS control-word on the ASR 9000.

- CSCud09813

  Symptoms: Timestamping not happening in CFM over xconnect down mep/PC

  Conditions: When we configured cfm over xconnect down mep/PC from Asr903-Me3600 timestamping not happening in ASR903.

  Workaround: No workaround.

- CSCud22601

  Symptom: MPLS-TP tunnels remain down after the standby RSP boots.

  Conditions: Occurs when you boot the standby RSP after applying an MPLS-TP configuration and performing an SSO. The issue occurs rarely.

  Workaround: Issue a shutdown/no shutdown on the MPLS-TP tunnel. A nonintrusive workaround is to cause a flap on the protect label switched path (LSP) by reconfiguring the path or physically shutting down and restoring the interface.

- CSCud23647

  Symptom: BDI adjacency fails on the standby RSP.

  Conditions: The issue can occur during an interface module (IM) reset or router reload.

  Workaround: There is no workaround.

- CSCud25764

  Symptoms: 903 part id to be populated in the discovery messages.

  Conditions: Currently it is being displayed as "cisco, asr903" against Vendor in host by executing this CLI "show nv satellite protocol discovery interface Bundle-Ether1000". This must be displayed as cisco, ASR-903. This is mainly used by ASR9K ACT tool for rendering 903 graphic on Act tool.

  Workaround: No workaround.

- CSCud26812

  Symptom: The router CLI does not display some SFP PIDs

  Conditions: Occurs when you install one of the following SFPs in the router:

  - ONS-SI-155-L2
  - ONS-SI-155-L1

  - ONS-SI-155-I1

  Workaround: There is no workaround.

- CSCud27333

  Symptom: The router crashes continuously.

  Conditions: Occurs when you issue an interface module reset (OIR) while the standby RSP is booting.

  Workaround: Do not issue an interface module reset (OIR) while the standby RSP is booting.

- CSCud28982

  Symptom: The router does not process egress CoS marking on an Ethernet service instance.

  Conditions: Occurs when you configure QoS on an Ethernet service instance that is a member of a bridge-domain and uses dot1q encapsulation.

  Workaround: There is no workaround.

- CSCud29479

  Symptom: The router stops applying QoS configurations.

  Conditions: Occurs under the following conditions:

  - An Ethernet interface is configured with a single service instance
  - A QoS policy is attached to the service instance
  - The QoS policy contains a single class containing a **match efp** statement.
  - You reset the interface to the default configuration.

  Workaround: There is no workaround.

- CSCud30806

  Symptoms: Policy with class map match-all with prec 1 and prec 2 is accepted for WRED.

  Conditions: match-all should not accept 2 prec values class-map match-all prec1_2 match precedence 1 match precedence 2

  Workaround: N/A

- CSCud33298

  Symptom: The router crashes.

  Conditions: Occurs when the peer device shuts down.

  Workaround: There is no workaround.

- CSCud33906

  Symptom: Equal Cost Multipath (ECMP) loopback does not function properly.

  Conditions: Occurs when a port-channel link dynamically assigned as an ECMP path.

  Workaround: There is no workaround.

- CSCud34346

  Symptom: Nile manager crashes with the ECMP path when IPv4 scale is exceeded.

  Conditions: This symptom occurs when scale is exceeded with the ECMP path.

  Workaround: Do not allow the user to exceed the supported IPv4 route scale with ECMP.

- CSCud34600

Symptom: Receive a event hog msg when advertise 21k to 25 k routes into MBGP and export from a PE to other PE.

Conditions: When the redistributing routes from range of 21k to 25k customer routes from ospf into MBGP and export from a PE to other PE.

Workaround: No workaround as of now.

- CSCud35689

  Symptoms: Queue-limit configuration at parent level of a policy or in a Vlan class/ port level is accepted. It should be rejected

  Conditions: When configuring queue limit on policy at parent level or in vlan class/ port level.

  Workaround: None

- CSCud36014

  Symptoms: Multiple entries are seen in configs

  Conditions: while configuring licence in bootlevel

  Workaround: -none-

- CSCud37927

  Symptoms: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

  Conditions: If we have REP or STP on core with one port as ALT or BLK state.

  Workaround: None.

- CSCud38038

  Symptom: The router records incorrect delay measurements after a reload.

  Conditions: Occurs under the following conditions:

  - You configure Delay Measurement Message (DMM) on a port-channel interface.
  - The port-channel member links are on different interface modules (IMs).
  - You reload the router.

  Workaround: You can use the following workarounds:

  - Remove the **ethernet cfm global** command and re-apply it after the port-channel member links recover.
  - Configure PTP clock synchronization.

- CSCud38115

  Symptom: OSPF connections flap and drop traffic for approximately 20 seconds

  Conditions: Occurs during stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCud38433

  Symptom: The router is unable to establish MPLS neighborship or ping the destination loopback interface.

  Conditions: Occurs when you configure two Equal Cost Multipath (ECMP) paths on a bridge domain interface (BDI) using static routes.

  Workaround: The following workarounds exist:

  - Use Interior Gateway Protocol (IGP) instead of static IP routes.

  - Shut down one of the ECMP paths.

- CSCud38589

  Symptoms: DMM Session Stops Working

  Conditions: DMM configured on BD UP MEP, with redundant links on the Core side, which are in STP Fwding / Blocked state, Issue seen when the STP Fwd Port is shut.

  Workaround: restart the IP SLA session or unshut the port and bring it FWD state

- CSCud38880

  Symptoms: IPv6 traffic drop post SSO with MetroIP services license.

  Conditions: 1. Start bidirectional IPv6 traffic on ASR903 with dual RSP and MetroIP services license, 3.7.1a. Put at least 3-4 streams each running at 10Mbps 2. Force switchover " redundancy force switchover" 3. IPv6 traffic will drop for 4-5 seconds. If you see drops in few milliseconds, then try adding more traffic. Issue is consistently recreatable.

  Workaround: Upgrade the license to MetroAgg, add v6 static neighbor on the port facing test set and force switchover, now there will be no ipv6 traffic loss.

- CSCud41217

  Symptoms: Multicast traffic dropped on 903.

  Conditions: The following l2 configuration are there. There are 3 satellites connected in the setup, only 903 satellite interfaces are showed here.All interfaces are in the same bridge domain. When sent the mcast traffic from 2/4, it is expected that all the satellite interface would received the traffic. But the two 903 satellite interfaces didn't receive the traffic, the other interfaces from other satellite were fine.

  2/4 --------gi0/3/0/11 PE1 gi400/0/2/1 --------3/2 gi400/0/3/1 --------7/4 ..... (901, 9000v satellite interfaces are omitted)

  2/4 sent (225.1.1.1, 192.10.1.1) at the rate of 2000 pps.

  Workaround: No workaround.

- CSCud44768

  Symptom: Multilink bundles and member links flap when passing traffic.

  Conditions: Occurs under the following conditions:

  - You configure more than 210 MLPPP bundles with one member link per bundle or 16 bundles with 16 member links each.
  - The line is operating at a 64 or 128 byte line rate

  Workaround: There is no workaround.

- CSCud48356

  Symptoms: Nile Manager crash seen while configuring service instance

  Conditions: After applying mpls tp config on back to back consoles

  Workaround: There is no workaround.

- CSCud50944

  Symptom: The router drops traffic on an MLPPP bundle.

  Conditions: Occurs following a reload while the router is passing traffic close to the line rate. The issue occurs less frequently with lower traffic rates.

  Workaround: Issue a **shutdown/no shutdown** on multilink interface.

- CSCud55377

  Symptom: The router crashes.

  Conditions: Occurs when you configure offloaded CFM for xconnect sessions at a high scale.

  Workaround: There is no workaround.

- CSCud55695

  Symptom: When you apply an QoS policy with a port level class-default configuration containing a shaper value to a serial interface. the router applies the shaper value to the channel-level PIR for all serial interfaces on the IM.

  Conditions: Occurs when you apply QoS policy with a port level class-default configuration containing a shaper value to a serial interface.

  Workaround: Add a dummy class-default level at the top of the policy and apply the shaper as a child policy of this class.

- CSCud55799

  Symptoms: Multiple priority commands get accepted per policy

  Conditions:

  Have a policy-map with priority configured in one of its classes. add another class with policer first and then with priority. this policy must be rejected.

  Workaround: none

- CSCud56262

  Symptom: The router stops passing traffic on virtual circuits.

  Conditions: Occurs an MPLS-TE/FRR configuration with L2VPN after you issue a stateful switchover (SSO).

  Workaround: Reload the router.

- CSCud56364

  Symptoms: Convergence time for POS links for rsp SSO is about 4-7 seconds.

  Conditions: All 4 POS links must be created on OC3IM. Issue not seen on port 0 of OC3IM.

  Workaround: None. Expected to be fixed.

- CSCud60410

  Symptom: The router drops EFP traffic.

  Conditions: Occurs when you add a new EFP to an existing bridge domain interface (BDI) while running L3 multicast.

  Workaround: Issue a **shutdown/no shutdown** on the Ethernet interface and issue the **clear ip mroute** command.

- CSCud64034

  Symptoms: Interfaces not coming up

  Conditions: 1) Configure t1 interfaces 2) Verify ping & they are coming up 3) Perform SSO 4) Verify Ping again & traffic 5) Unconfigure t1 interfaces .6) Reload the standby 7) Configure t1 interfaces 8) T1 interfaces are not coming up

  Workaround: IM OIR on box

- CSCud64129

Symptoms: Control-plane policing is not working on ASR903; despite CLI showing the options to do it: ASR903(config)#control-plane ASR903(config-cp)#service-policy ? input Assign policy-map to the input of an interface output Assign policy-map to the output of an interface

Conditions: Using traditional CoPP CLI to restrict CPU punted traffic

Workaround: This is a not a supported feature on ASR903.

Further Problem Description: ASR903 has an implicit policer to protect different kinds of traffic destined to RP's CPU. By default, they are policed up to 1Mbps. This is tunable as well. For more details:
http://www.cisco.com/en/US/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-punt-police-monitor.html This software defect is a means to get the unsupported CLI removed from the IOS-XE.

- CSCud64347

  Symptom: The router creates a data loop when using a REP VLAN load balancing configuration.

  Conditions: Occurs with a REP VLAN load balancing configuration when a bridge-domain is bound to a VPLS VC.

  Workaround: None; remove the VLAN load balancing configuration.

- CSCud64436

  Symptom: The router does not send the full line rate on POS interfaces.

  Conditions: Occurs when you send traffic over a POS interface on the OC-3 interface module with a QoS configuration.

  Workaround: There is no workaround.

- CSCud64923

  Symptom: OSPF connections flap.

  Conditions: Occurs when you configure OSPF between an EVC bridge domain interface (BDI) and a trunk EFP bridge domain interface (BDI) using a port-channel trunk.

  Workaround: There is no workaround.

- CSCud65779

  Symptom: The router does not update the Rx value for C2, J1, and S1S0 bytes.

  Conditions: Occurs when you configure overhead bytes on OC-3 connections.

  Workaround: There is no workaround.

- CSCud71286

  Symptoms: Config Sync Failures seen with respect interface.

  Conditions: when AutoNeg is disabled on the interface and configured with speed 100/1000

  Workaround: There is no Functionality impact.No Workaround.

- CSCud71546

  Symptom: The ten Gigabit Ethernet interface drops traffic for 7 seconds following a stateful switchover (SSO).

  Conditions: Occurs when the configuration contains static routes to the destination.

  Workaround: There is no workaround.

- CSCud74804

  Symptoms: Building of rudy_satellite_super image failed. **Conditions:** While building rudy_satellite_super image, not able to find some subsystem and build failed. **Workaround:** No Workaround.

- CSCud76209

  Symptom: The OC-3 interface module goes into an out of service state.

  Conditions: Occurs when you repeatedly perform an interface module reset (OIR) on the OC-3 interface module.

  Workaround: There is no workaround.

- CSCud76679

  Symptom: The router displays a serial interface in the mroute table but does not forward traffic over the assigned interface.

  Conditions: Occurs when you enable multicast traffic on the OC-3 interface module.

  Workaround: There is no workaround.

- CSCud76770

  Symptoms: Convergence time for FRR link/node protection is more than 2 seconds.

  Conditions: NNHOP backup tunnels configured in a ring topology.

  Workaround: No workaround.

- CSCud78168

  Symptoms: Higher convergence (>5 seconds) is observed for 3107 label imposition prefixes.

  Conditions: With 3107 label imposition configured.

  Workaround: No workaround

- CSCud83069

  Symptom: End-to-end traffic does not flow for ATM PVP Mode.

  Conditions: Occurs when you enable ATM PVP Mode.

  Workaround: There is no workaround.

- CSCud83698

  Symptom: Links on the Gigabit Ethernet interface do not become active.

  Conditions: Occurs on the Gigabit Ethernet interface when the local interface is configured for autonegotiation and the remote interface is configured for a speed of 10 Mbps or 100 Mbps.

  Workaround: Toggle the auto-negotiation configuration on the Gigabit Ethernet interface.

- CSCud89451

  Symptom: The router crashes with an error message showing nmpls_label_populate_flow_data.

  Conditions: Occurs when you reset a core interface while the ASR 903 is acting as a PE router and running a configuration with L2VPN and L3VPN.

  Workaround: There is no workaround.

- CSCud90362

  Symptoms: PTP master (OC/BC) on ASR903, the SYNC packets might go out quite irregularly.

  Conditions: This is seen with ASR903 is configured as PTP master.

Workaround: There is no workaround.

Further Description: This depends a lot on the slave and its tolerance levels with respect to SYNC packets reception and processing. With most of the vendors and Test tools it works today except few.

- CSCud90890

  Symptoms: Routing over Trunk EFP over Port-channel doesn't work on member ports associated with Asic #1

  Conditions: If a Trunk EFP on Port-channel has members on asic#1, routing traffic won't egress on those ports

  Workaround: None

- CSCud92915

  Symptoms: Enable BFD support for IPFRR in 3.8.1

  Conditions: BFD with IPFRR

  Workaround: There is no workaround.

- CSCud95359

  Symptom: The show policy map command displays an incorrect number of total dropped packets (total drops).

  Conditions: Occurs when you issue the show policy-map command to display dropped packets on an interface.

  Workaround: There is no workaround.

- CSCud96604

  Symptoms: On system reset/reload, all traffic on certain EFPs will not egress

  Conditions: Complete traffic stoppage on certain EFPs

  Workaround: Delete and reconfigure EFPs

- CSCud96962

  Symptoms: After shut/noshut the mem link interface getting tracebacks - IM Flapping

  Conditions: Configured cfm trunk efp pc -256 session -3.3ms interval after that shut/no shut the traffic sending interface will hit this issue

  Workaround: Configure very less session 50-100 cfm session

- CSCud98985

  Symptoms: on executing show tech-support, invalid command errors were detected for a few commands

  Conditions: on executing show tech-support, invalid command errors were detected for a few commands

  Workaround: There is no workaround.

- CSCud99183

  Symptoms: Ctrl protocols stay down, pings fail on booting with scaled ACE/ACL, (ACL configurations are failing)

  Conditions: it occurs only on reload time

  Workaround: There is no workaround.

- CSCue00049

Symptoms: classification not works properly with non-matching traffic when IP acl is used.

Conditions: This occurs only if we have classes based on acl match. only acl class will classify properly and other classes based on dscp or class-default wont work

Workaround: No known workaround

- CSCue00332

  Symptom: BFD connections flap, bringing down IGP.

  Conditions: Occurs when you enable BFD on an interface that is flapping.

  Workaround: There is no workaround.

- CSCue01419

  Symptoms: EIGRP neighborship is lost on OC3IM / OC12 IM interfaces configured on port 0.

  Conditions: Seen only for interfaces which are configured on port 0 of OC3IM or OC12 IM. Not seen on ports 1,2 or 3.

  Workaround: Perform a shut/no shut on interfaces configured on port 0. Alternatively remove EIGRP and configure again.

- CSCue01919

  Symptoms: Enhancement to L2 protocol tunnelling feature to forward/drop more protocols and reserved mac addresses that are under IEEE wellknown mac address range (0180C2000002-0F) as a part of CE2.0 certification.

  Conditions: This the L2 protocol tunnelling enhancement for CE2.0 certification.

  Workaround: There is no workaround.

- CSCue03418

  Symptoms: The router displays OSPF protocol flaps causing a 20–30 second traffic loss.

  Conditions: The issue occurs very intermittently on a HA system with a 6 second dead-interval value when you issue the **redundancy force-switchover** command;

  Workaround: Increase the dead-interval value.

- CSCue05962

  Symptoms: Cos/Vlan Classification doesn’t work on port channel member links

  Conditions: Apply a Cos based Qos policy on port-channel member links. All the packets will start flowing through class default instead of getting classified on the interface. Look at the attached console logs for configs details.

  Workaround: None

- CSCue07849

  Symptoms: Link failure in L3VPN core takes a long time (in 10s of seconds) to converge even with BGP PIC enabled.

  Conditions: BGP PIC core and PIC edge is configured and there are more than one ECMP core paths to reach backup BGP peer.

  Workaround: Configure only one core path to reach both primary and repair BGP Peers in a BGP PIC Core + Edge configuration. If these are more than one equal cost physical paths to reach BGP peers, then adjust the configuration by increasing the distance for all paths except one.

Post fix caveat: With the fix for this issue, there are following limitations on the scale of prefixes: 1. Global labeled BGP prefix scale: 3200 2. VPN (with or without labeled-BGP nexthop) prefix scale: 4000 3. Combination of Global labeled BGP and VPN prefix: less than 3200 depending on number of VPN and number of labeled BGP prefixes.

- CSCue11444

  Symptoms: Split horizon configurations doesn't work on nile 1 with L2 multicast packets

  Conditions: EFPs with split-horizon configured on nile 1 doesn't honor SH conditions (remain just using deja vu)

  Workaround: shut/no shut. Configure EFP first before moving into split-horizon group.

- CSCue16617

  Symptoms: QoS classification not working in core

  Conditions: When Output policy applied to interface having the BDI as core interface.

  Workaround: Enable "mpls ldp explicit null" on all the Routers.

- CSCue16828

  Symptoms: b2b ping is not working - core side trunk efp PC with BDI

  Conditions: when we have core side trunk efp pc with BDI and changed the port channel in core side b2b ping is not working.

  Workaround: Don‘t change the PC in core side.

- CSCue17123

  Symptoms: ATM/IMA Ping Fails From 2nd Interface Post SSO In xe39 nightly.

  Conditions: This is seen when you have multiple ATM interfaces and issue switchover. Traffic doesn't flow from 2nd interface after switchover.

  Workaround: No workaround

- CSCue18015

  Symptoms: No S,G created. Forwarding based on (*,G).

  Conditions: Happens with IGP change leading to RPF change of the (*,G).

  Workaround: Clearing th (*,G) and recreating should help fixing the problem.

  Further Problem Description: Timing issue and hence chances of landing into the problem depends on the events getting triggered.

- CSCue19898

  Symptoms: (*,G) based forwarding can be seen with IIF change. IGP patch change to the source might lead to this problem.

  Conditions: If the IGP change, the RPF change notification comes. In that case we miss adding the cpuq to the (*G).

  Workaround: Timeout the (*,G) entry and recreating it again either by clear ip mroute or stopping the joins.

- CSCue20022

  Symptoms: -Core (S, G) entries will software switch with-out any hardware forwarding

  Conditions: -IIF is PIM enabled BDI interface. -Scale EVCs configured under single port -Scale BDIs as IIFs -Trigger: Flap main interface having EFPs

Workaround: -Clear Multicast Routes for failing (S, G) -Soft IM OIR for failing IIF interface having scale EVCs

- CSCue24621

  Symptoms: when we do shut on one of the efp, traffic gets stop for other evcs also

  Conditions: Where there are multiple qinq efps with same outer vlan tag on one interface.

  Workaround: None.

- CSCue25267

  Symptoms: Stand-by rsp reloads on IM OIR on OC3IM on active rsp. Nile manager crash seen but core file incompletely generated.

  Conditions: Seen when active rsp is booted up first, then standby rsp is booted. With serial links and APS configs on ASR903, perform IM OIR.

  Workaround: None.

- CSCue25567

  Symptoms: quack authentication failure msg seen on console.

  Conditions: It is seen randomly.

  Workaround: Reload the router.

- CSCue26927

  Symptoms: Alarms are not forwarded in CEM.

  Conditions: Alarms are not forwarded when AC goes down.

  Workaround: No Workaround.

- CSCue27652

  Symptoms: ATM interfaces getting deleted on SSO

  Conditions: ATM Interfaces are deleted on standby after IM OIR

  Workaround: No Workaround.

- CSCue27922

  Symptoms: Syslog showing Object download for the prefix and traffic will not flow for the particular prefix.

  Conditions: Issue is seen during multiple interface flap with 4K prefix and rLFA enabled.

  Workaround: Reload the router

- CSCue30481

  Symptoms: The router does not lock to the syncE clock source after reload. It will be in Ql-failed state.

  Conditions: Reload the router with saved syncE configuration.

  Workaround: Unconfigure and configure the clock source.

- CSCue32753

  Symptoms: While performing ISSU, the OC3IM interfaces are lost on ISSU completion. This is followed with config mismatch errors on router console. When new stand-by reaches standby-hot state, continuous iomd crash messages are seen at regular intervals.

  Conditions: Seen when ISSU is performed from older label images to XE39 image.

Workaround: None. Unconfigure controller level OC3 configs and configure again. To stop continuous iomd crash, reload the standby rsp once. If IM went into inserted or out of service state, then a HARD OIR or process kill might be required.

- CSCue34597

  Symptoms: CHAP authentication process timed out. PPP interface and multilink bundle doesn't come up.

  Conditions: When PPP or MLPPP is configured and PPP authentication is enabled.

  Workaround: remove CHAP authentication from interface

- CSCue34618

  Symptoms: Traffic stops flowing with combination of BRR and policer: in different class-maps under a policy.

  Conditions: When the BW remaining ratio is configured in combination of police with cir (total brr and police cir equal to 1000M):

  Workaround: Configuring total of BRR and police cir <1000M works fine: Ex: class A Police cir 100m and class B BRR 90% fails but BRR 89% works fine

- CSCue35356

  Symptoms: Policy-map attached on the PC interface stops working after service instance is removed and re-configured.

  Conditions: A policy-map is attached to the main interface of the port-channel. The policy stops working when the service instance from the interface is deleted dynamically and then re-configured.

  Workaround: Remove and re-attach the policy-map on the PC interface

- CSCue36239

  Symptoms: Match EFP policy on PC stops working after one of the policy on the member links is removed.

  Conditions: Attach policy to all the memberlinks on the PC. Then remove it from one of the member links from which traffic was flowing. The traffic gets redirected but the QoS is no longer working

  Workaround: Remove policy from all the member links and then reattach

- CSCue43205

  Symptoms: The router drops traffic when you set an interface to the default configuration.

  Conditions: Occurs when you set an interface with QoS configurations to

  the default configuration. The issue occurs most often with the Ten Gigabit

  Ethernet interface using a full global configuration.

  Workaround: There is no workaround.

- CSCue42315

  Symptoms: CPU Hogs messages and IOMD Crash seen

  Conditions: With OC3 IM on doing shut/no shut of Multilink Bundle when traffic sent with packet size greater then 1500 byte

  Workaround: none

- CSCue42341

  Symptoms: Backup path will be used to carry traffic instead of Primary path after reopt

  Conditions: R-LFA + BFD needs to be configured together

Workaround: Flap the backup path interface

- CSCue43250

  Symptoms: IMA config won't be parsed correctly after router reload when the A903-IM40S is inserted in Bay4/Bay5 of the ASR903 router

  Conditions: when the IMA and ATM interfaces are adjacent. happens only for IM inserted on Bay 4 or above.

  Workaround: insert the IM in bay 0 bay 3 if you want the IMA and ATM parsing to work. or reconfigure the ATM and IMA interfaces, it would work.

- CSCue45306

  Symptoms: CEM circuits configured over TDM IM go down after SSO.

  Conditions: on SSO, CEM circuits configured over TDM IM are down.

  Workaround: Router reload.

- CSCue45498

  Symptoms: CPU goes high when sending traffic with varying source mac addresses for multiple streams for BD.

  Conditions: port-channel is configured as efp for the BD and mac-limit is configured to 0 for that BD.

  Workaround: N/A

- CSCue47317

  Symptoms: Builds and ISSU may get impacted due to sync damage in latest throttles with respect to CCO data.

  Conditions: Modification in implementation of TDL structures.

  Workaround: Sync with CCO data will be committed shortly.

- CSCue52774

  Symptoms: observed with A900-IMA4OS IM in ASR903 box. only when the port above 0 is used for clock-source, the clocking is not received by the system correctly.

  Conditions: when the port above 0 is used for the clock source. issue is seen due to wrong conversion.

  Workaround: 1. use port 0 for clock-sync 2. or insert the SFP in the odd port(protect ones) adjacent to actual port and using a optical splitter, the cable can be fed to this odd port which can recover the proper clocking for the given port.

- CSCue52968

  Symptoms: Ping fails and traffic stops through Multilink bundle when CHAP authentication is enabled

  Conditions: This is seen when PFC and ACFC is configured.

  Workaround: None, in case PFC and ACFC is configured.

- CSCue57670

  Symptoms: After SSO without any network-clock config new Active RSP Sync LED reflects Holdover state.

  Conditions:

  Workaround: Reload This is a cosmetic issue.

- CSCue57671

  Symptoms: Router Crashes while running with REP configurations **Conditions:** Crash seen while removing REP configuration from interface. **Workaround:** None

- CSCue59544

  Symptoms: Once path is once available for TE tunnel, it doesn't comes up **Conditions:** If A900-IMA16D is also present on router, it generates storm which prevent RSVP processing and TE tunnel doesn't up once TE path is available again

  Workaround: None

- CSCue77612

  Symptoms: The mac sync can happen on wrong lportid in the standby which can cause traffic forwarding to the wrong port after switchover.

  Conditions: The traffic impact will be seen only after the switchover.

  Workaround: clear mac-add after switchover.

- CSCue86696

  Symptoms: Noticed interface flap on one of the routers, during overnight soak run.

  Conditions: Seen during prolonged soak tests with SFP IM.

  Workaround: None

- CSCue87542

  Symptoms: On BDI delete, if routing traffic continues, it will be punted to the CPU which will flood out the CPU resulting in control plane loss

  Conditions: Ping failure and BFD/OSPF flaps on BDI delete while ipv4/v6 traffic is running.

  Workaround: The workaround is to delete the TEFP and then delete the BDI interfaces.

- CSCue89790

  Symptoms: IPv6 traffic outage after SSO when NSF timer expires.

  Conditions: Occurs when configuring IPv6 static routing or IPv6 OSPF routing.

  Workaround: For IPv6 SSO support, ensure the following:

  - IPv6 neighbor are configured statically.
  - For dynamic route or static route, you must run a hardware BFD between IPV6 neighbors.

Restrictions and Caveats in Cisco IOS XE 3.10 Releases

This chapter provides information about restrictions and caveats in Cisco IOS XE 3.10 releases.

Note We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

This chapter contains the following sections:

Limitations and Restrictions

The following limitations apply to the Cisco ASR 903 Router in IOS XE Release 3.10(0)S:

TDM Limitation

- The **configure replace** command is not supported for TDM interfaces.

IPv6 Limitations

The following limitation applies when using IPv6 on the Cisco ASR 903 Router:

- IPv6 Neighbor Discovery (ND) cache timer expiry is 4 hours. To prevent the neighbor adjacency from being deleted after the timer expires:
  - configure hardware based BFD sessions with the neighbors, or
  - configure static IPv6 neighbors, or
  - configure the **ipv6 nd cache expire timer refresh** command.

OC-3 IM Limitations

- The **configure replace** command is not supported on the OC-3 IMs.

Caveats in Cisco IOS XE 3.10S Releases

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in this chapter.

This section describes caveats in Cisco IOS XE 3.10S releases. The following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

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.

Caveats

The following sections describe the open and resolved caveats in 3.10S Releases:

- Open Caveats—Cisco IOS XE Release 3.10.2S, page 6-3
- Resolved Caveats—Cisco IOS XE Release 3.10.2S, page 6-4
- Open Caveats—Cisco IOS XE Release 3.10.1S, page 6-8
- Resolved Caveats—Cisco IOS XE Release 3.10.1S, page 6-11
- Open Caveats—Cisco IOS XE Release 3.10S, page 6-16
- Resolved Caveats—Cisco IOS XE Release 3.10S, page 6-19

Open Caveats—Cisco IOS XE Release 3.10.2S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 router in Cisco IOS XE Release 3.10.2S.

- CSCuf15863

  Symptom: Traffic loss of few milliseconds seen on the router.

  Conditions: This issue occurs when remote LFA is configured on the core, and on shuting a primary path, the site which is not on primary path gets some milli second loss.

  Workaround: There is no workaround.

- CSCuf35464

  Symptom: The active bits port does not send out the QL properly which is received from the remote bits.

  Conditions: This issue occurs when the remote bits are configured as input and active bits as output.

  Workaround: There is no workaround.

- CSCui74718

  Symptom: %EVENTLIB-3-RUNHOG tracebacks are reported on the console.

  Conditions: This issue occurs when the router is configured in PTP slave mode. The clock is in phase aligned state and PTP configurations are removed using the **no ptp clock ordinary domain** command.

  Workaround: There is no workaround.

- CSCul07048

  Symptom: IPv6 nd cache expire after reload or IM OIR is performed.

  Conditions: This issue occurs when ISIS with BFD is enabled on the BDI interface.

  Workaround: Reload or replace the configuration.

- CSCul50165

  Symptom: The router fails to forward packets with the maximum configured MTU.

  Conditions: This issue was observed on MLPPP, T1, POS interfaces when the **mtu** *max MTU* **interface** command was executed on the router.

  Workaround: There is no workaround.

- CSCul58083

  Symptom: After IP mtu is configured on an interface, any change in to the MTU are not reflected on the interface.

  Conditions: This issue occurs when IP mtu is configured and the MTU is changed.

  Workaround: Set the required interface MTU before executing the **ip mtu** command or unconfigure the IP MTU on the interface and then change the interface MTU.

- CSCum40613

  Symptom: The TOD port on the router does not function when configured as slave.

  Conditions: This issue occurs after configuring TOD on the router.

  Workaround: There is no workaround.

- CSCum47925

  Symptom: SSO convergence time of ~0.9 sec is observed with 100m SFP.

  Conditions:This issue occurs when VPLS VC and EVC BD exists on the access.

  Workaround: There is no workaround.

- CSCum79011

  Symptom: Pending objects take a long time (approx 30 min) to clear on the router.

  Conditions: This issue occurs when QoS-policy is applied on member-link and services like psuedowire, HSRP on BDI are configured on the port-channel.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.10.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.10.2S.

- CSCuf35542

  Symptom: PFM fails for about 5minutes after OIR on the master.

  Conditions: This issue occurs after OIR is triggered two times on the master

  Workaround: Wait for 5-6 minutes

- CSCuh06123

  Symptom: QL-mapping displays incorrectly on master.

  Conditions: This issue occurs when QL value is configured first and then PTP master is configured

  Workaround: Reconfigure QL values or reload the router.

- CSCuh49073

  Symptom: OSPF does not come up when PIM is enabled on the VPLS core interface.

  Conditions: This issue occurs when PIM is enabled on the VPLS core interface.

  Workaround: There is no workaround.

- CSCuh54159

  Symptom: Packet drops are seen under QOS policy map attached on the multilink bundle for traffic rate less than bundle capacity

  Conditions: This issue occurs when unexpected packet drops are seen for QOS for traffic rates less than bundle bandwidth. After reloading the router with QOS policy attached on bundle, packet prioritization into different queues with differing bandwidth profiles occurs.

  Workaround: Remove and reattach the policy map on the bundle

- CSCui41169

  Symptom: Active card reloads when standby comes active after switchover with scaled configuration

  Conditions: This issue occurs when 4000K EVCs with 1-level ingress policy, and 2-level egress policy is configured on the router. Ingress policy should have 1-level policer, egress policy should have one parent and child policer. The issue occurs after a reload of the card with this configuration.

  Workaround: There is no workaround.

- CSCui44409

Symptom: No console message are seen on insertion or removal of USB

Conditions: This issue is observed standby RSP.

Workaround: More Info:

- CSCui45075

  Symptom: When an IM is removed from the router, the MST states are not reflected in the standby RSP. If a switchover happens at this state, it could cause total traffic drop.

  Conditions: This issue is seen when HA is configured on the router.

  Workaround: There is no workaround.

- CSCui98883

  Symptom: System crashes on configuring TOD.

  Conditions: This issue occurs on dual RSP setup and PTP is configured.

  Workaround: There is no workaround.

- CSCui99309

  Symptom: IPv6 BFD with static client does not display when VRF is configured.

  Conditions: This issue occurs when VRF is configured on the router.

  Workaround: There is no workaround.

- CSCuj30644

  Symptom: Multicast does not function in scaled mode and when BDI is configured on the core.

  Conditions: This issue was seen in the scaled mode.

  Workaround: Execute the **no ip igmp snooping** command on the router to forward the multicast traffic.

- CSCuj34652

  Symptom: IPv6 traffic drops for the packets with next header options. Next header options include Hop-by-hop options, fragment header.

  Conditions: This issue occurs when option packets are punted to CPU and generates the time exceeded message.

  Workaround: There is no workaround.

- CSCuj38988, CSCum45935

  Symptom: QL does not move to QL-FAILED state when the Gigabit ethernet interface is shutdown.

  Conditions: This issue occurs when the Gigabit ethernet interface is shutdown.

  Workaround: There is no workaround.

- CSCuj42208

  Symptom: Layer3 multicast traffic drop is seen on Trunk port.

  Conditions: This issue occurs when multicast is converged. Performing a **shutdown** followed by a **no shutdown** on the multicast router interface fails to transmit multicast traffic to TEFP's.

  Workaround: Clear IP multicast routes using **clear ip mroute** command for IPv4 traffic and **clear ipv6 pim topo** command for IPv6 traffic.

- CSCuj43453

  Symptom: IOSd crash was seen on the router on bootup of PTP process.

  Conditions: This issue occurs during bootup when multiple reloads of the router is performed.

  Workaround: There is no workaround.

- CSCuj43795

  Symptom: The port in error-disabled state & physical status shows as down but is UP on the other connected end device.

  Conditions: This issue occurs when the port is configured with DHCP rate limiting values so that the port goes to error-disable state once it reaches the rate configured.

  Workaround: Perform a **shutdown** followed by a **no shutdown** on the respective interface to move the port to UP state.

- CSCuj60116

  Symptom: SYNC-E does not get synced in WAN mode.

  Conditions: This issue occurs in WAN mode.

  Workaround: There is no workaround.

- CSCuj60771

  Symptom: Self-generated DHCP traffic generating out of the router is not getting marked (cos) with user specified value.

  Conditions: This issue occurs when DHCP packets (CPU to client) are not getting marked.

  Workaround: There is no workaround.

- CSCuj96689

  Symptom: **Queue-limit** command is not programmed for priority queue.

  Conditions: This issue occurs when the policy map has both BRP and Priority queue with queue-limit configured for priority queue.

  Workaround: Perform the following;

  - Attach the policy with all BRP configuration.
  - Dynamically add the **queue-limit** command to the priority class.

- CSCul10279

  Symptom: Crash observed on the router with multicast VPN configuration.

  Conditions: This issue occurs when the router is configured with multicast VPN IPv4 configuration, Scaled ACL and IGMP Static Join configuration.

  Workaround: There is no workaround.

- CSCul11877

  Symptom: HSRP standby router cannot ping the virtual IP.

  Conditions: This issue occurs when the BDI interfaces are configured along with a range of bridge domains.

  Workaround: There is no workaround.

- CSCul21294

  Symptom: PTSF alarms do not get posted when the egress interface is shutdown.

  Conditions: This issue occurs when a PTP slave has one or more masters.

Workaround: There is no workaround.

- CSCul21429

  Symptom: The router console freezes and the OSPF or BFD sessions flap.

  Conditions: This issue occurs when TOD type is changed dynamically on a PTP master from NTP to Cisco or vice-versa.

  Workaround: Unconfigure TOD and reconfigure a new TOD type.

- CSCul21447

  Symptom: The ANNOUNCE message does not get updated.

  Conditions: This issue occurs in the PTP slave.

  Workaround: There is no workaround.

- CSCul40676

  Symptom: Ping failure observed on the interface connected with port 0/0/0 with ACR configuration.

  Conditions: This issue occurs when ACR is configured on the router.

  Workaround: Install the IM in the other bay or change the port other than 0/0/0 as the core.

- CSCul46353

  Symptom: Traffic drop observed on priority queues.

  Conditions: This issue occurs on QoS policy with 2-level priority queues (priority level classes) that do not guarantee the bandwidth on 1-level priority against 2-level traffic.

  Workaround: There is no workaround.

- CSCul46643

  Symptom: Convergence with SSO for REP with multicast is greater than 3 seconds.

  Conditions: This issue occurs on performing an SSO on the Receiver

  Workaround: There is no workaround.

- CSCul49147

  Symptom: Time exceed message is generated when IPv6 packets are received on the router.

  Conditions: This issue occurs when IPv6 packets have option headers.

  Workaround: If the IPv6 options have fragment header then increase the MTU size.

- CSCul50181

  Symptom: A Cisco router may see unicast traffic not being forwarded out of the Gigabit ethernet interface while multicast traffic is being processed by the router correctly.

  Conditions: This issue occurs when the router has BDI configured to the Gigabit ethernet interface.

  Workaround: Reload the router.

- CSCul51784

  Symptom: IPv6 packets fails to get forwarded out of the router.

  Conditions: This issue occurs when unicast RPF enabled for IPv4 traffic and IPv6 traffic is received on the interface.

  Workaround: Remove unicast RPF checks on the interface where dual stack is configured.

- CSCul52778

  Symptom: STM -1 port keeps on increasing on changing the **card type** command multiple times.

Conditions: This issue occurs after executing the card type command many times.

Workaround: There is no workaround.

- CSCul65485

  Symptom: Wrong speed and bandwidth is displayed with DWDM XFP

  Conditions: This issue occurs when the DWDM XFP is inserted and the **show interface** command is executed.

  Workaround: There is no workaround.

- CSCul65977

  Symptom: Enabling DAI on one interface leads to ARP packets being dropped on another interface in the same BD or xconnect.

  Conditions: This issue occurs after enabling DAI on one interface.

  Workaround: There is no workaround.

- CSCul80289

  Symptom: Crash observed on the router.

  Conditions: This issue occurs after unconfiguring the BDI interface and TEFP is learnt as mrouter.

  Workaround: There is no workaround.

- CSCum02924

  Symptom: PTP session gets stuck in unknown state.

  Conditions: This issue occurs when OSPF, clock domain & clock source are unconfigured and reconfigured.

  Workaround: There is no workaround.

- CSCum42701

  Symptom: Tx and Rx power does not display the right values for OC-3 SFP.

  Conditions: This issue is seen when the controller is disabled and the SFP is inserted.

  Workaround: Perform a hard OIR of the OC-3 SFP.

Open Caveats—Cisco IOS XE Release 3.10.1S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 router in Cisco IOS XE Release 3.10.1S.

- CSCue42139

  Symptom: The ptp state is stuck in acquiring state all the time

  Conditions: This issue occurs when the active RSP is removed; the T3 timestamping is stuck and the ptp state stays in acquiring state all the time.

  Workaround: Unconfigure and configure the ptp.

- CSCuf78234

  Symptom: The **queue-limit** command displays packets as default.

  Conditions: This issue occurs when **queue-limit** command is configured on the router.

  Workaround: Configure queue-limit is microseconds (us) or bytes.

- CSCug97269

  Symptom: The serial interface flaps when the neighbor controller is shut.

  Conditions: This issue occurs occurs on performing shutdown on peer OC-3 controller with ATM or IMA channels.

  Workaround: There is no workaround.

- CSCuh83433

  Symptom: The path level controllers status on OC-3 IM sonet controller is not displayed after a second SSO is triggered manually after removing the RSP.

  Conditions: This issue is seen on hard RSP reset of RSP1.

  Workaround: Perform a controller **shutdown** followed by a **no shut down**.

- CSCui08697

  Symptom: The interface LED glows green after SSO.

  Conditions: This issue occurs after an SSO is performed and shut down of the ports on the router.

  Workaround: There is no workaround.

- CSCui34041

  Symptom: Traffic does not flow on one of the prefix of the MPLS template.

  Conditions: This issue occurs when the MAX MPLS label of that template is assigned to that prefix

  Workaround: Disable and enable that prefix.

- CSCui41169

  Symptom: The active card reloads when standby become active after switchover with scaled configurations.

  Conditions: This issue occurs with 4000 EVCs with first and second level ingress policy. The Ingress policy has one policer and the egress policy has one parent and child policer. This issue occurs with reloading the card with this configuration.

  Workaround: There is no workaround.

- CSCui53268

  Symptom: Adding a child policy map with Vlan class to parent PHB class dynamically, does not trigger the error message.

  Conditions: This issue occurs when a PHB level policy is attached to an interface and any policy is being dynamically added as a child to one of the existing PHB classes.

  Workaround: Detaching the policy and performing a modification and trying to reattach displays the error.

- CSCui62568

  Symptom: No error reported when invalid policer is dynamically modified to remove the PIR configuration with violate-action.

  Conditions: This issue occurs when a policy-map with CIR and PIR value attached to an EFP is dynamically modified to just CIR which make the policer have exceed action without PIR.

  Workaround: Remove the violate-action first and then remove PIR configuration.

- CSCui74718

  Symptom: "%EVENTLIB-3-RUNHOG" tracebacks reported on the console.

  Conditions: This issue occurs on the router in ptp slave mode. The clock is in phase aligned state and the ptp configurations are removed using the **no ptp clock ordinary domain** command.

  Workaround: There is no workaround. There is no functional impact.

- CSCui92961

  Symptom: 100% traffic loss is observed on few pseudowires.

  Conditions: This issue occurs when the router experiences couple of link flaps.

  Workaround: Issue **shutdown** command followed by **no shutdown** command on the EFP; this can be tedious if impacted pseudowire count is more.

- CSCuj04299

  Symptom: FMAN FP core traceback observed on the router.

  Conditions: This issue occurs after adding several new EFPs or BDIs to running configuration and updating the QoS configuration on the physical interface

  Workaround: There is no workaround.

- CSCuj09392

  Symptom: Dynamically modifying the user-defined to class-default triggers error.

  Conditions: This issue was seen when modifying the user-defined to class-default.

  Workaround: There is no workaround.

- CSCuj32391

  Symptom: Dynamic modify of parent with class default policer to child policer does not take effect.

  Conditions: This issue occurs on dynamic modify DM of parent having class-default policer value greater than child policer value.

  Workaround: Reattach the policy-map

- CSCuj38988

  Symptom: Queue-limit does not go to queue-limit failed state when we the gigabit ethernet interface is shutdown.

Conditions: This issue occurs while shutting down he gigabit ethernet interface.

Workaround: There is no workaround.

- CSCuj51830

  Symptom: Traffic drops if policy is attached on port-channel interface.

  Conditions: This issue occurs when the policy is attached on port-channel interface

  Workaround: Use port-channel IDs less than 10.

- CSCuj56164

  Symptom: TCAM utilization shows incorrect current usage percentage.

  Conditions: This issue occurs when EQoS application is enabled.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.10.1S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.10.1S.

- CSCue60699

  Symptom: Router auto negotiates full duplex with 1000M half/full duplex configuration.

  Conditions: This issue occurs when a router with Copper SFP with auto-negotiating is enabled and the peer router with Cu SFP configured with 1000M half-duplex mode exists.

  Workaround: There is no workaround.

- CSCug31550

  Symptom: Incorrect TCAM entries with scale configuration are displayed after reapplying the policy map.

  Conditions: This issue occurs after removing the policy map and reapplying it to service instances.

  Workaround: There is no workaround.

- CSCug36190

  Symptom: Object Download failures are seen when configuring xconnect on the main interface and configure xconnect under the service instance.

  Conditions: This issue occurs when xconnect is configured on the main interface.

  Workaround: Remove the xonnect configuration from the main interface.

- CSCug50280

  Symptom: QoS does not work on the router.

  Conditions: This issue occurs while adding user class to a port level policer dynamically when the policer already has class-default configured.

  Workaround: Reload the router.

- CSCug68820

  Symptom: The **show inventory** command does not display PSU and fan tray information.

  Conditions: This issue occurs after the PSU or fan tray is inserted after bootup and SSO is performed.

  Workaround: Reload after PSU or the fan tray after it is inserted.

- CSCug70182

  Symptom: The ASR903-IMA8S port remains up without the fiber.

  Conditions: This issue occurs when the GLC-FE-100FX optic is used.

  Workaround: There is no workaround.

- CSCug96284

  Symptom: Memory leaks seen on boot up of the router.

  Conditions: This issue occurs on booting the system.

  Workaround: There is no workaround.

- CSCuh00108

  Symptom: CMAND crash seen on the router.

  Conditions: This issue occurs during midplane idprom read at bootup.

  Workaround: Reload the router.

- CSCuh03023

  Symptom: IP connectivity over BDI fails after a link flap network event.

  Conditions: This issue occurs intermittently with BDI enabled for IP/MPLS forwarding and running VPN services over it. Adjacency failures are seen after couple of link flap events, which impacts Layer3 forwarding over BDI.

  Workaround: There is no workaround.

- CSCuh13883

  Symptom: Standby IOMD crashes continuously at system bootup.

  Conditions: This issue occurs at system bootup and when the system waits for a user input at the initial dialog box during configuration.

  Workaround: There is no workaround.

- CSCuh16707

  Symptom: The interface module (IM) status LED glows green before the PHY Init state is complete.

  Conditions: This issue occurs after an IM OIR is performed.

  Workaround: Use the **show platform** command output to check if the IM reaches the OK state.

- CSCuh42926

  Symptom: High CPU utilization is seen when Trunk EFP is configured on port channel and MAC address table limit is configured on the bridge domain.

  Conditions: This issue occurs when Trunk EFP is configured on port channel and MAC address table limit is configured on the bridge domain.

  Workaround: Do not use port channel.

- CSCuh46103

  Symptom: BDI statistics not getting incremented on the router.

  Conditions: This issue occurs when the ingress and egress statistics displayed using **show interface bdi** or the **show int bdi statistics** command does not get incremented even if the traffic is flowing through the BDI interface.

  Workaround: Use **show platform hardware pp active interface statistics bdi** command to view the statistics.

- CSCuh51651

  Symptom: CPP download failures and CFM remote MEPS not learnt.

  Conditions: This issue occurs during configuring CFM offload scaled configurations using TFTP.

  Workaround: There is no workaround.

- CSCuh51702

  Symptom: The system shuts down after 5mins irrespective of ambient temperature after removing the fan tray.

  Conditions: This issue occurs after removing the fan tray.

  Workaround: There is no workaround.

- CSCuh81135

  Symptom: Port speed configuration is changed automatically on changing the SFP module.

  Conditions: This issue occurs on changing the SFP module.

  Workaround: There is no workaround.

- CSCuh85990

  Symptom: Some CFM MEPs are not learnt when configuring large number (about 1K) on the router.

  Conditions: This issue is seen only if large number of MEPs are configured.

  Workaround: Remove and re-apply the configuration.

- CSCuh92939

  Symptom: Traffic drop occurs after replacing a Cu SFP with a fiber FP

  Conditions: This issue occurs after replacing Cu SFP with fiber SFP after an SSO is performed.

  Workaround: Perform an IM OIR.

- CSCuh99117

  Symptom: Packet drops for some of the prefixes in MPLS network are observed.

  Conditions: This issue occurs when MPLS Layer3 VPN is configured on the router with MVPN template.

  Workaround: There is no workaround.

- CSCui16418

  Symptom: After a switchover is performed, the ten gigabit ethernet interface might flap and traffic drops.

  Conditions: This issue occurs after SSO is performed.

  Workaround: There is no workaround.

- CSCui32127

  Symptom: CFM download error-objects are observed when CFM peers are reloaded or IM OIR is done on a scaled VPLS and CFM setup.

  Conditions: This issue occurs on the router with 250 or more CFM MEP sessions and more than 1250 Layer2 virtual circuit sessions.

  Workaround: There is no workaround.

- CSCui34041

  Symptom: Traffic does not flow to one of the prefix on MPLS template.

Conditions: This issue occurs when maximum MPLS label of that template is assigned to that prefix.

Workaround: Disable and enable the prefix.

- CSCui40994

  Symptom: Ethernet CFM ping fails because remote MEPs are not learnt.

  Conditions: This issue occurs when MIP is configured on the same Vlan as MEP on the CFM domain.

  Workaround: Remove MIP configuration.

- CSCui50577

  Symptom: Traffic drops are observed on router.

  Conditions: This issue occurs after performing an IM OIR.

  Workaround: There is no workaround.

- CSCui58365

  Symptom: Router reboots while modifying a policy-map with class-map "**match vlan 100**".

  Conditions: This issue occurs while attaching the "**match vlan 100**" egress policy-map. This issue occurs after adding an ingress policy with no-match class and then adding an egress policy with **match** on Vlan or dynamically adding match vlan class on egress policy.

  Workaround: There is no workaround.

- CSCui68159

  Symptom: Traffic drops when two EFPs are configured on with default encapsulation and **rewrite push do1q** on same BD.

  Conditions: This issue occurs when two EFPs are configured on with default encapsulation and **rewrite push do1q** on the same BD.

  Workaround: There is no workaround.

- CSCui87339

  Symptom: Transceiver init_failure observed after transceiver OIR is performed.

  Conditions: This issue is seen after the OIR of transceiver is performed.

  Workaround: A slow OIR of transceiver might recover the port.

- CSCui93830

  Symptom: HQoS top level service-policy fails on the router when switching between the RSPs.

  Conditions: This issue occurs when switching between the RSPs.

  Workaround: Reattach the policy-map.

- CSCuj07507

  Symptom: High convergence for downstream traffic observed on the router.

  Conditions: This issue occurs when VPLS VFI's is controlled by g.8032 open ring, with a large scale of about 500VC's and 10000 MAC (40 per BD).

  Workaround: Use small MAC scales for traffic.

- CSCuj42080

  Symptom: The FGPA gets stuck while pumping high volume of CFM packets.

  Conditions: This issue occurs while pumping high volume of CFM packets on the router.

Workaround: There is no workaround.

- CSCuj50260

  Symptom: CFM ping fail to MPIDS on the router.

  Conditions: This issue occurs when MEPS are configured over port channel.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.10S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 router in Cisco IOS XE Release 3.10S.

- CSCue36365

  Symptom: During initial bootup of the serial interface module, the first character of the first packet received might be missing.

  Conditions: Problem occurs during a cold boot of the serial interface module.

  Workaround: There is no workaround. Problem is a transient condition and traffic resumes after receipt of the first message on the module.

- CSCue42144

  Symptom: PHY stops timestamping and the session stays at acquiring state.

  Conditions: This issue is observed when you insert the Cu-SFP on the slave.

  Workaround: There is no workaround.

- CSCue49537

  Symptom: The Cisco ASR 903 router crashes when you perform an OC3 IM OIR.

  Conditions: This issue is observed when you have about 700 CEM circuits and perform an OC3 IM OIR.

  Workaround: There is no workaround.

- CSCue87629

  Symptom: The following error message is displayed:

  ```
  INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client 'iosd-nile'
  ```

  Conditions: This issue is observed when you use the **shutdown** and **no shutdown** commands on the G8032 ring interface of peer or local device.

  Workaround: There is no workaround.

- CSCuf16426

  Symptom: FMAN_FP download fails and the following error message is displayed:

  ```
  %CHUNK-2-BADREFCOUNT errors.
  ```

  Conditions: Have an MPLS TE in the core and flap the tunnels intermittently.

  Workaround: Do not flap the core TE tunnels often.

- CSCug15175

  Symptom: The Cisco ASR 903 router falsely displays the following error message saying that a BFD node is down:

  ```
  %OSPF-5-ADJCHG: Process 232, Nbr 192.0.2.33 on BDI632 from FULL to DOWN, Neighbor
  Down: BFD node down
  ```

  Conditions: This issue is observed when you configure a BFD software session.

  Workaround: There is no workaround.

- CSCug36590

  Symptom: The Cisco ASR 903 router displays the following error message:

  ```
  %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex for an interface on the
  Standby, allocating a new ifindex from the Active (ifindex=126, idbtype=SWIDB)
  ```

  Conditions: This issue is observed when you create an ATM channel, create a POS link, or create DS3 links.

  Workaround: There is no workaround.

- CSCug43550

  Symptom: The receiver node crashes when the number of traffic sources increases beyond 400 with 196 OIFs at the receiver end.

  Conditions: This issue is observed when 196 IGMP packets are sent to a node per second.

  Workaround: Reduce the number of IGMP packets to four per second.

- CSCug84082

  Symptom: Ping fails and traffic drops on ATM/IMA PVP links configured on either T1E1 IM or OC3 IM.

  Conditions: This issue is observed when you perform an SSO and flap the ATM/IMA link.

  Workaround: Perform an IM OIR or reload the router.

- CSCug96003

  Symptom: When operating with a large number of TCP Raw Socket connections (greater than 512) and with traffic on all of them we saw some TCP retransmissions.

  Conditions: The issue occurred in a stress test within a lab setup.

  Workaround: None required.

- CSCuh06123

  Symptom: QL mapping is incorrect on the PTP master.

  Conditions: This issue is observed when you first reboot the router or configure and unconfigure the router multiple times.

  Workaround: Reconfigure the Ql values.

- CSCuh33291

  Symptom: The Cisco ASR 903 router generates linkDown traps when an interface changes from administratively down state to down state.

  Conditions: This issue is observed when an interface changes from administratively down state to down state.

  Workaround: There is no workaround.

- CSCuh33314

  Symptom: When you perform an ISSU or terminate the IOMd process, IOMd crashes on the standby RSP.

  Conditions: This issue is observed when you terminate the IOMd process on the active RSP or when you perform an ISSU.

  Workaround: There is no workaround.

- CSCuh81658

Symptom: Although a QoS policy is configured, PTP packets are treated as default packets.

Conditions: This issue is observed when the CPU-generated PTP packets do not reach egress QoS with high a priority label (15 or 126).

Workaround: There is no workaround.

- CSCuh85041

  Symptom: SNMP returns the wrong card type for the serial interface module.

  Conditions: Issue occurs during SNMP walk of ASR903.

  Workaround: There is no workaround. This issue is not service affecting.

- CSCuh85990

  Symptom: When you use the **show ethernet cfm maintenance-points remote** command, only 992 remote maintenance endpoints are displayed.

  Conditions: This issue is observed when you configure CFM MEP domains on an EVC.

  Workaround: There is no workaround.

- CSCuh88500

  Symptom: Standby router reloads due to SPA bulk synchronization failure.

  Conditions: This issue is observed when you perform an SSO.

  Workaround: There is no workaround.

- CSCui06748

  Symptom: ICMP packets are punted to the CPU even after using the **no ip redirect** command on the Cisco ASR 903 router.

  Conditions: This issue is observed when ICMP packets are punted initially.

  Workaround: There is no workaround.

- CSCui14481

  Symptom: Traffic does not flow for HSPW sessions as the tunnel ID is incorrect.

  Conditions: This issue is observed when you perform an IM OIR.

  Workaround: Perform an SSO and flap the access interface.

- CSCui19632

  Symptom: BFD sessions flap randomly.

  Conditions: This issue is observed in FPGA version 30020.

  Workaround: There is no workaround.

- CSCui19700

  Symptom: When you apply a QoS policy on the core interface, QoS counters do not increment.

  Conditions: This issue is observed when you apply a policy on the access interface with 500 EFPs and apply another policy on the core interface.

  Workaround: There is no workaround.

- CSCui22637

  Symptom: The Cisco ASR 903 router crashes.

  Conditions: This issue is observed when you unconfigure 1000 Ethernet service instances.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.10S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.10S.

- CSCtx70302

  Symptom: Traceback and log messages are seen while performing a multilink bundle shutdown on the Cisco ASR 903 router.

  Conditions: This issue is observed when traffic flows over the multilink bundle.

  Workaround: There is no workaround. This issue does not impact the operation of the router.

- CSCua61934

  Symptom: When a policy map with priority in class-default is attached to an interface, it is not rejected.

  Conditions: This issue is observed when you configure policy-map having priority in class-default and attach the policy to an interface.

  Workaround: There is no workaround.

- CSCua90879

  Symptom: QoS policies with a police statement on the class-default class do not take effect.

  Conditions: This issue is observed when you apply a police statement to the class-default class within a QoS policy on an ingress EVC interface.

  Workaround: Apply the police statement to a static class, such as class cos0.

- CSCuc59386

  Symptom: IOMD crashes continuously on OC-3 IM. The interfaces on OC-3 IM are not configurable and the following error message is displayed:

  ```
  stand-by does not support this command
  ```

  Conditions: This issue is observed on a Cisco ASR 903 router high availability setup with OC-3 IM.

  Workaround: Reload the standby RSP.

- CSCuc60148

  Symptom: The router does not shut down when the temperature sensor reaches the shutdown threshold.

  Conditions: Temperature sensor reaches shutdown threshold.

  Workaround: Use the **facility-alarm critical exceed-action shutdown** commands to enable system shutdown.

- CSCuc83088

  Symptom: The router drops traffic while performing a Stateful Switchover (SSO).

  Conditions: This issue is observed when the router is running HSRP or VRRP. It occurs when the destination MAC address is a virtual MAC (vMAC) address.

  Workaround: Change the traffic priority and detour traffic before performing an SSO.

- CSCud09100

  Symptom: The router accepts a policy with marking at two levels. It should not accept a policy with marking at two levels.

  Conditions: This issue is observed when you apply a policy with marking at two levels.

Workaround: There is no workaround.

- CSCud09813

  Symptom: Timestamping does not work in CFM over cross-connected MEP with port channel.

  Conditions: This issue is observed when you configure CFM over cross-connected MEP with port channel from a Cisco ASR 903 router to a Cisco ME 3600 switch.

  Workaround: There is no workaround.

- CSCud12624

  Symptom: Traceback is displayed when you configure the ACR group.

  Conditions: This issue is observed when you configure an ACR group.

  Workaround: There is no workaround.

- CSCud29491

  Symptom: A two-level policy with match EFP in parent and PHB-based policy in child can be applied.

  Conditions: This issue is observed when you apply a policy on a physical interface having EFPs on that physical interface.

  Workaround: There is no workaround. This configuration is not supported.

- CSCud34630

  Symptom: The following error message is displayed on the standby machine while using the **shutdown** and **no shutdown** commands on the ACR controller:

  ```
  NETWORK_RF_API-3-FAILDECODEDATADESC
  ```

  Conditions: This issue is observed on the standby machine when you configure ACR interface.

  Workaround: There is no workaround.

- CSCud35689

  Symptoms: The router accepts a queue-limit configuration at the parent level of a policy or at the vlan class or port level.

  Conditions: This issue is observed when you add a queue-limit configuration on a policy at the parent level or at the vlan class or at port level.

  Workaround: There is no workaround. This configuration is not supported.

- CSCud35732

  Symptom: The router does not apply egress CFM MIP filtering.

  Conditions: This issue is observed when you overwrite a MIP configuration using the ethernet CFM MIP level command.

  Workaround: Instead of overwriting the MIP level configuration, remove and reapply the configuration.

- CSCud38038

  Symptom: The router records incorrect delay measurements after a reload.

  Conditions: This issue is observed under the following conditions:

  - You configure Delay Measurement Message (DMM) on a port-channel interface.
  - The port-channel member links are on different interface modules (IMs).
  - You reload the router.

Workaround: Remove the **ethernet cfm global** command and reapply it after the port-channel member links to bundle. Alternatively, configure PTP clock synchronization.

- CSCud38833

  Symptom: When you configure the ACR CEM interfaces, tracebacks are displayed and the serial interface remains down.

  Conditions: This issue is observed when you create a second CEM circuit under the same controller and delete the CEM circuit immediately.

  Workaround: There is no workaround.

- CSCud41297

  Symptom: Multicast snooping traffic drops after removing and reconfiguring the querier EFP on 1000 groups.

  Conditions: This issue is observed when you remove and reconfigure querier EFP with more than 500 multicast routs.

  Workaround: There is no workaround.

- CSCud43718

  Symptom: After performing an SSO, multicast traffic is dropped for a few groups.

  Conditions: This issue is observed in a scaled configuration with IGMP snooping enabled in a bridge-domain.

  Workaround: There is no workaround.

- CSCud55695

  Symptom: When you apply a QoS policy with a port level class-default configuration containing a shaper value to a serial interface, the router applies the shaper value to the channel-level PIR for all serial interfaces on the IM.

  Conditions: This issue is observed when you apply a QoS policy with a port level class-default configuration containing a shaper value to a serial interface.

  Workaround: Add a dummy class-default level at the top of the policy and apply the shaper as a child policy.

- CSCud55799

  Symptom: Multiple priority commands are accepted per policy.

  Conditions: This issue is observed when you have a policy map with priority configured in one of its classes. Add another class with policer first and with priority.

  Workaround: There is no work around.

- CSCud56364

  Symptom: Convergence time for POS links for RSP SSO is about four to seven seconds.

  Conditions: This issue is observed when all four POS links are created on OC-3 IM. This issue is not observed on port 0 of OC-3 IM.

  Workaround: There is no work around.

- CSCud61551

  Symptom: The serial number of the RSP in slot 1 is sometimes not displayed in the **show inventory** command output.

  Conditions: This issue is sometimes observed in the **show inventory** command output.

  Workaround: Reload the router.

- CSCud64129

  Symptom: The router displays command options to configure control-plane policing, which is not supported.

```
Router(config)# control-plane
Router(config-cp)# service-policy ?
input Assign policy-map to the input of an interface
output Assign policy-map to the output of an interface
```

  Conditions: This issue is observed when you attempt to configure control plane policing to restrict traffic by the CPU.

  Workaround: There is no workaround. This feature is not supported.

- CSCud71286

  Symptom: Configuration synchronization failure is noticed on the interfaces.

  Conditions: This issue is observed when you disable autonegotiation and configure the interface speed as 100 or 1000.

  Workaround: There is no workaround. There is no impact on functionality.

- CSCud90457

  Symptoms: The serial interface on the CE end connected to the CEM interfaces on PE remain down on router reload with scaled configuration.

  Conditions: This symptom is observed when you have CESoP and SAToP scaled circuits and reload the router.

  Workaround: Perform an IM OIR to resolve the issue.

- CSCud93007

  Symptom: If you use the command **channel-group 1 mode active** on a interface, the router does not reject the command.

  Conditions: This issue is observed after you configure a trunk EFP MEP using the **ethernet cfm mep domain v7 mpid 1537 service v7137** command on an interface.

  Workaround: There is no workaround.

- CSCud96866

  Symptom: The router displays the following symptoms:

  - Object download failures.
  - OSPF traffic flaps.
  - High CPU utilization.
  - Bundling and unbundling of port-channel member links.
  - Slow console updates.
  - Remote MEP learning failures.

  Conditions: This issue is observed when you configure CFM offloaded MEPs on a port-channel interface at a high scale and use the **shutdown** and **no shutdown** command on the port-channel interface.

  Workaround: There is no workaround.

- CSCue00045

  Symptom: Data traffic drops for a few groups when you use the **shutdown** and **no shutdown** commands on the interface.

  Conditions: This issue is observed if join request is sent to the router within three minutes.

  Workaround: There is no workaround.

- CSCue01419

  Symptom: EIGRP neighborship is lost on OC3IM and OC12 IM interfaces configured on port 0.

  Conditions: This issue is observed only on interfaces that are configured on port 0 of OC3IM or OC12 IM. It is not seen on ports 1,2, or 3.

  Workaround: Use the **shutdown** and **no shutdown** commands on the interfaces configured on port 0. Alternatively, remove and reconfigure EIGRP.

- CSCue03418

  Symptoms: Intermittently OSPF protocol flaps are noticed when you use the **redundancy force-switchover** or the **switchover** command. It can cause about 20 to 30 seconds of traffic loss.

  Conditions: This symptom is observed while performing an SSO or when using the **redundancy force-switchover** command and on a HA system with 6 seconds as OSPF dead interval.

  Workaround: Increase the dead interval value.

- CSCue07040

  Symptom: The router continuously displays ESDHC and MMCBLK0 errors.

  Conditions: This issue is observed when the SD flash memory is being accessed.

  Workaround: There is no workaround. Replace or format the bootflash.

- CSCue14054

  Symptom: When a port joins more number of multicast groups at a time, traffic drops for a few groups.

  Conditions: This issue is observed when a port joins more than 900 multicast groups.

  Workaround: Use the **shutdown** and **no shutdown** commands on that interface.

- CSCue17123

  Symptom: ATM and IMA pings fail from the second interface after performing an SSO.

  Conditions: This issue is observed when you have multiple ATM interfaces and perform a switchover.

  Workaround: There is no workaround.

- CSCue18997

  Symptom: In unicast mode, the PTP slave stream does not lock to the PTP master.

  Conditions: This issue id observed after the PTP master configuration is removed and reconfigured.

  Workaround: There is no workaround.

- CSCue25146

  Symptom: When the controller in active machine flaps, the standby machine is reloaded.

  Conditions: This issue is observed when you configure ATM and the controller, use **shutdown** and **no shutdown** commands on the controller in the active machine.

  Workaround: There is no workaround

- CSCue27652

  Symptoms: The ATM interfaces are deleted while performing an SSO.

  Conditions: This issue is observed when the ATM interfaces are deleted on the standby machine after performing an IM OIR.

  Workaround: There is no workaround.

- CSCue30481

  Symptom: The router does not lock to the syncE clock source after a reload. It is in Ql-failed state.

  Conditions: This issue is observed when you reload the router with a saved syncE configuration.

  Workaround: Delete and reconfigure the clock source.

- CSCue35295

  Symptom: Traffic drops when you remove the BFD template.

  Conditions: This issue is observed when you remove the BFD template from the global configuration.

  Workaround: There is no workaround.

- CSCue36239

  Symptom: Match EFP policy on a port channel stops working after one of the policies on the member links is removed.

  Conditions: This issue is observed when you attach a policy to all the member links on the port channel, remove it from one of the member links from which traffic flows.

  Workaround: Remove policies from all the member links and reattach the policies.

- CSCue39978

  Symptom: Traffic stops in ATM PVP after performing an IM OIR followed by SSO.

  Conditions: This issue is observed after performing an IM OIR followed by SSO when ATM PVP is configured.

  Workaround: Reload the router.

- CSCue43250

  Symptom: IMA configuration is not parsed correctly after a router reload when the A903-IM40S module is inserted in Bay4 or Bay5 of the Cisco ASR 903 router.

  Conditions: This issue is observed when the IMA and ATM interfaces are adjacent. It happens only if the IM is inserted on Bay 4 or above.

  Workaround: Insert the IM in bay 0 or bay 3 if you want the IMA and ATM parsing to work. Alternatively, reconfigure the ATM and IMA interfaces.

- CSCue45274

  Symptom: Traffic drop is seen on a port for more than 8 minutes when a BDI, which is not part of this new port is shut down.

  Conditions: This issue is observed when a BDI is shut down and another port which is not a part of the shut down BDI port join the multicast group.

  Workaround: There is no workaround.

- CSCue45306

  Symptom: The CEM circuits that are configured over TDM IM go down after performing an SSO.

  Conditions: This issue is observed when you perform an SSO, the CEM circuits that are configured over TDM IM go down.

  Workaround: Reload the router.

- CSCue47834

  Symptom: IOMd crashes and IM goes out of service during SSO.

  Conditions: This issue is observed when you have ATM and IMA configured and perform an SSO. IOMd crashes and the IM goes out of service.

  Workaround: There is no workaround.

- CSCue54997

  Symptom: The system accepts two input clock sources from the same OC3 IM although the system supports only one input clock source per OC3 IM. This results in clock failures.

  Conditions: This issue is observed when two input clock sources are accepted from the same OC3 IM although the framer on the IM can support only one clock source.

  Workaround: Do not configure the second input clock source from the same OC3 IM. Alternatively, remove both OC3 clock sources and configure the desired OC3 controller.

- CSCue57671

  Symptom: Router crashes while running the REP configuration.

  Conditions: This issue is observed while removing the REP configuration from the interface.

  Workaround: There is no workaround.

- CSCue66019

  Symptom: The router displays MLPPP interface errors.

  Conditions: This issue is observed when there is more than 90% line rate traffic with mix MTU patterns.

  Workaround: There is no workaround.

- CSCue67835

  Symptom: OSPF flaps when you set the dead interval timer as 6 seconds and hello interval as 2 seconds.

  Conditions: This issue is observed when you perform an SSO.

  Workaround: Use the default OSPF hello timers.

- CSCue72481

  Symptom: The same interface accepts an IP address and a MEP.

  Conditions: This issue is observed when you configure an IP address and a MEP to the same interface.

  Workaround: There is no workaround.

- CSCue83621

  Symptom: Policy map stops working after you dynamically remove class default class.

  Conditions: This issue is observed when the policy map is attached to the target and the class default of the top level is deleted dynamically, the policy stops working.

  Workaround: Detach and reattach the policy map on the target.

- CSCue89503

  Symptom: The power supply status reports critical after you remove and insert the power supply.

  Conditions: This issue is observed after performing multiple OIRs.

  Workaround: There is no workaround.

- CSCuf01120

  Symptom: IOMD crash is seen while performing an SSO when card type is not configured for T1E1 IM.

  Conditions: This issue is observed when the TDM card type is not configured before performing an SSO.

  Workaround: Configure the card type for T1E1 IM before preforming an SSO.

- CSCuf20151

  Symptom: The following error message is displayed when you apply a policy map:

  ```
  QoS: Configuration failed. Can NOT match ACL in an output policy-map
  ```

  Conditions: This issue is observed when you apply a policy map, reload, or reconfigure of the policy map.

Workaround: There is no workaround.

- CSCuf43275

  Symptom: The router does not detect traffic through GLC-FE-100EX and GLC-FE-100ZX transceivers.

  Conditions: The router does not support traffic through GLC-FE-100EX and GLC-FE-100ZX transceivers.

  Workaround: There is no workaround.

- CSCuf43992

  Symptom: The router crashes if you configure local span.

  Conditions: This issue is observed when you configure local span on the router.

  Workaround: There is no workaround.

- CSCuf44077

  Symptom: The **show interface** command output shows incorrect speed values after performing an SSO.

  Conditions: This issue is observed when you use a 100M SFP.

  Workaround: There is no impact on functionality. Reset the hardware module to resolve this issue.

- CSCuf57632

  Symptoms: When you reload the router, the device may not be able to load the startup configuration from NVRAM.

  Conditions: This issue is sometimes observed when you reload the router.

  Workaround: Reload the router again.

- CSCuf65012

  Symptom: When you perform an IM OIR on slot 4, the router may display syslog messages from the GigabitEthernet 0/5/0 port.

  Conditions: This issue is observed when you perform an IM OIR on slot 4 and Slot 5.

  Workaround: There is no workaround.

- CSCuf79364

  Symptom: When you try configure speed on the interface on the standby machine, it does not accept the command.

  Conditions: This issue is observed after you insert a new IM and GE-T connector when router is running.

  Workaround: Reload the router before configuring the speed.

- CSCuf79504

  Symptom: When you use the **shutdown** and **no shutdown** commands multiple times on the controller, ATM VC creation on the standby RSP fails.

  Conditions: This issue is observed when you use the **shutdown** and **no shutdown** commands multiple times on the controller on active RSP.

  Workaround: There is no workaround.

- CSCuf81085

  Symptom: After you use the **shutdown** and **no shutdown** commands on the controller of PE, IMA VCs go down.

  Conditions: This issue is observed after using the **shutdown** and **no shutdown** commands on the OC3 controller on PE routers.

  Workaround: Use the **shutdown** and **no shutdown** commands on the controller.

- CSCuf85460

  Symptom: When you delete the POS interface and try to create an ATM interface, the following error message is displayed:

  ```
  %OC3.STS1 0/2/0.1:Port type not supported
  Insufficient resources to create channel group
  ```

  Conditions: This issue is observed when you reload the OC3-IM having POS interface and try to create an ATM interface.

  Workaround: Create the POS interface, delete it, and the create an ATM interface.

- CSCuf89665

  Symptom: Flow control identifiers of active and protect interfaces are not created on to the standby. Due to which, the interface goes down when you perform an SSO.

  Conditions: This issue is observed when you set up ACR on the standby machine.

  Workaround: There is no workaround.

- CSCuf89844

  Symptom: The router crashes when you delete a BDI interface running BFD.

  Conditions: This issue is observed when you assign a static MAC address on a neighbor router or on one of the BDI interfaces on the Cisco ASR 903 router, and delete the BDI interface running BFD on the Cisco ASR 903 router.

  Workaround: There is no workaround. Do not change the MAC address on the BDI interface.

- CSCug16135

  Symptom: Critical alarm LED does not illuminate. The **show facility-alarm status** command shows a critical alarm.

  Condition: This issue occurs when both active and standby RSP are in UP state.

  Workaround: Use the **show facility-alarm status** command to view the alarm status.

- CSCug17844

  Symptom: Traffic does not match the configured class map of the applied policy.

  Conditions: This issue is observed at egress, if a policy map which contains 8 user-defined class-maps is applied. As it exceeds the allowed number of class maps, traffic hits the class default.

  Workaround: Remove the 8th user-defined class map and reapply the policy.

- CSCug18630

  Symptom: When you perform an OIR on the standby and active RSPs, CMAND crashes.

  Conditions: This issue is observed after performing multiple standby OIRs and bringing the standby machine up.

  Workaround: There is no workaround.

- CSCug31212

  Symptom: When you apply a policy map, the console shows an error message.

  Conditions: This issue is observed when you apply a policy map with numbered ACLs.

  Workaround: There is no workaround.

- CSCug31645

  Symptom: If you change the template on the router and change it again within two minutes, the standby RSP is unable to synchronize with the new template and the router reloads twice.

  Conditions: This issue is observed when you change the template, and change it again within two minutes before reloading the router.

  Workaround: Do not change the template and change it again within two minutes.

- CSCug44762

  Symptom: The POS interface stays down after using the **shutdown** and **no shutdown** commands.

  Conditions: This is issue is observed when you use the **shutdown** and **no shutdown** commands on the POS interface.

  Workaround: Use the **shutdown** and **no shutdown** commands on the controller.

- CSCug48534

  Symptom: Multicast traffic is forwarded on untagged EFPs when snooping is enabled.

  Conditions: This issue is observed when untagged EFPs are shutdown at least once after it comes up.

  Workaround: Reload the router or toggle IGMP snooping.

- CSCug55586

  Symptom: If you dynamically remove the egress markings, ingress marking does not work.

  Conditions: This issue is observed if a marking is present at the logical level in the egress direction, DM does not work.

  Workaround: Use the egress set at leaf or PHB level.

- CSCug58606

  Symptom: When you use the **no shutdown** command, the LED of 1G and 10G IM turns off.

  Conditions: This issue is observed when you use the **no shutdown** command on 1G and 10G interfaces.

  Workaround: There is no workaround.

- CSCug61357

  Symptom: ISIS adjacency and BFD stay down after using the **shutdown** and **no shutdown** commands.

  Conditions: This issue is observed in R-LFA configurations.

  Workaround: Use the **shutdown** and **no shutdown** commands again.

- CSCug83426

  Symptom: Interface reports loss of frame alarm and goes down.

  Conditions: This issue is observed when you use the **shutdown** and **no shutdown** commands on the controllers of PE and CE.

  Workaround: Perform an OIR on CE side.

- CSCug83846

  Symptom: The MTU value does not take effect on an interface.

  Conditions: This issue is observed when you try to configure more than eight unique MTU values on the router.

  Workaround: There is no workaround.

- CSCug94540

  Symptom: The total drop counters on an interface is not displayed when HQoS policy map is applied.

  Conditions: This issue is observed when you apply a two-level policy on a port.

  Workaround: Use the **show policy-map interface gigabitethernet 0/0/0** command or **show hqf interface gigabitethernet 0/0/0** command.

- CSCug96958

  Symptom: IMA interfaces stay up even when you use the **shutdown** command to shut down the controller.

  Conditions: This issue is observed when you use the **shutdown** command on the OC3 controller.

  Workaround: Use the no shutdown command bring up the controller and interfaces.

- CSCug99750

  Symptom: The Cisco ASR 903 router crashes when it accesses unpopulated data structures.

  Conditions: This issue is observed when you perform an IM OIR and use the **shutdown** and **no shutdown** commands.

  Workaround: There is no workaround.

- CSCuh00009

  Symptom: RSP crashes due to keepalive failure.

  Conditions: This issue is observed when the router is being polled from different SNMP servers at different intervals.

Workaround: Increase the SNMP polling interval.

- CSCuh06740

  Symptom: Router gets reloaded after performing a soft OIR.

  Conditions: This issue is observed after you perform a soft OIR or subsequent SSOs.

  Workaround: There is no workaround.

- CSCuh16011

  Symptom: FMAN-FP crashes when you perform ab IM OIR.

  Conditions: This issue is observed when you perform multiple IM OIRs with around 65 BFD sessions.

  Workaround: Reload the router.

- CSCuh18503

  Symptom: BFD IPv6 sessions may not come up between Cisco ASR 9000 and Cisco ASR 903 routers.

  Conditions: This issue is observed when the packets sent from Cisco ASR 903 router have invalid UDP checksums.

  Workaround: There is no workaround.

- CSCuh21696

  Symptom: When you disable IGMP snooping, the IGMP control packets are not flooded on all ports.

  Conditions: This issue is observed with TEFP over 10Gig, normal EFP, EFP over PC, and TEFP with IGMPSN.

  Workaround: There is no workaround.

- CSCuh27117

  Symptom: Traffic loss of about six to eight seconds is observed when you perform an SSO.

  Conditions: This issue is observed when you perform the switchover before IM OIR or the interface flaps.

  Workaround: There is no workaround.

- CSCuh48988

  Symptom: When you create a policy map the following error message appears:

  ```
  "Max class-maps in an Egress policy-map (port-channel_egress) cannot exceed 8"
  ```

  Conditions: This issue is observed when a policy map with more than 8 class maps is configured.

  Workaround: There is no workaround.

- CSCuh77762

  Symptom: On Cisco ASR 903 routers, the TenGigabitEthernet port operates at one gigabit speeds in WAN-PHY mode. This leads to a huge amount of output drop.

  Conditions: This issue is observed if a QoS policy is configured on the TenGigabitEthernet interface.

  Workaround: There is no workaround.

- CSCuh79730

Symptom: The transmitting frequency is incorrectly displayed in the output of the **show hw-module subslot 0 transceiver idprom** command.

Conditions: This issue is observed if you use DWDM-XFP-C modules.

Workaround: There is no workaround.

- CSCuh86102

  Symptom: The interface stops forwarding traffic

  Conditions: This issue is observed when the TenGigabitEthernet interface is in WAN-PHY mode and R0 is active.

  Workaround: Use R1.

Restrictions and Caveats in Cisco IOS XE 3.11 Releases

This chapter provides information about restrictions and caveats in Cisco IOS XE 3.11 releases.

Note We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Caveats in Cisco IOS XE 3.11S Releases

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in this chapter.

This section describes caveats in Cisco IOS XE 3.11S releases. The following information is provided for each caveat:

- Symptom—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

The following sections describe the open and resolved caveats in 3.11S Releases:

- Open Caveats—Cisco IOS XE Release 3.11S, page 7-2
- Resolved Caveats—Cisco IOS XE Release 3.11S, page 7-2

Open Caveats—Cisco IOS XE Release 3.11S

This section documents the unexpected behavior that might be seen with the Cisco ASR 903 router in Cisco IOS XE Release 3.11S.

- CSCuh86847

  Symptom: When MR-APS CEM feature is configured on the router, the traffic stops flowing on deletion and recreation of CEM groups and xconnects.

  Conditions: This issue occurs after deletion and recreation of CEM groups is performed and after a few iterations of performing an RSP SSO on a HA configured router..

  Workaround: Perform an OIR of the OC-3 IM to resume the traffic.

- CSCuj60116

  Symptom: WANPHY:SYNC-E does not gett synced in WAN mode.

  Conditions: This issue occurs in WAN mode.

  Workaround: There is no workaround.

- CSCul15030

  Symptom: Traffic drops for few seconds then resumes for 2-3 minutes.

  Conditions: This issue may be observed with a specific topology.

  Workaround: There is no workaround.

- CSCul21349

  Symptom: Crash is observed after seeing out of Tcam entries on the console.

  Conditions: This issue occurs after seeing out of Tcam entries on the console.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.11S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.11S.

- CSCuf35542

  Symptom: Precise Frequency Monitor (PFM) fails for about 5 minutes after OIR is performed.

  Conditions: This issue occurs after an OIR is trigger ed.

  Workaround: Wait for 5-6 minutes after an OIR.

- CSCug05491

  Symptom: The router drops traffic on VPLS circuits.

  Conditions: This issue occurs when REP is configured with VLAN load balancing and VPLS VFI is configured on the VLANs. This issue occurs after stateful switchover (SSO) is performed.

  Workaround: There is no workaround.

- CSCug39899

  Symptom: Traffic stops flowing go through QinQ BDI interface after ARP times out and the ARP is removed by shutting the BDI interface.

  Conditions: This issue occurs when static routing is configured and no routing protocol is configured on the interface.

Workaround: Manually resolve ARP by pinging the next hops BDI interface .

- CSCug44762

  Symptom: POS interface stays down after a **shutdown** followed by a **no shutdown** on POS interface.

  Conditions: This issue is seen when a **shutdown** followed by a **no shutdown** is performed on POS interface.

  Workaround: Perform **shutdown** followed by a **no shutdown** on the controller.

- CSCug50283

  Symptom: Only 2-path are utilized for load sharing though 3-path is available.

  Conditions: This issue occurs when ECMP is configured.

  Workaround: There is no workaround.

- CSCug61505

  Symptom: The **platform enable** command is seen for ACR virtual controller when OC-3 IM is present in slot 0.

  Conditions: This issue occurs after configuring aps group acr command on the OC-3 controller.

  Workaround: Insert the IM in other bays instead of bay 0.

- CSCug83434

  Symptom: Lot of memory leak chunks are seen for FMANRP on the standby RSP.

  Conditions: This issue occurs after memory leaks are verified on standby RSP.

  Workaround: Perform a router reload.

- CSCug84082

  Symptom: ATM/IMA PVP links configured on either T1/E1 IM or OC-3IM exhibit traffic or ping failure.

  Conditions: This issue occurs when ATM/IMA link flaps and is followed by SSO. Link flap can be IM OIR, etc.

  Workaround: Performing an IM OIR may fix the issue, else perform a router reload.

- CSCug84428

  Symptom: Traffic drop are seen on the T1/E1 IM serial and MLPPP links.

  Conditions: This issue occurs when traffic is sent via streams with jumbo packet sizes of 7000 bytes or larger. The interfaces toggle between the up/down state.

  Workaround: Perform a IM OIR of the T1/E1 IM.

- CSCug89348

  Symptom: IOSXE_RP_SPA-3-IPCPORTFAIL tracebacks are seen on router with high availability configured.

  Conditions: This issue occurs after SSO is performed.

  Workaround: There is no workaround.

- CSCug92536

  Symptom: PLATFORM-3-NOMAC traceback is seen on standby console.

  Conditions: This issue is seen when cem-acr is configured on a HA setup.

  Workaround: There is no workaround.

- CSCug96958

  Symptom: IMA interfaces stay up when controller is shutdown.

  Conditions: This issue occurs after performing an admin shutdown on OC-3 controller.

  Workaround: Perform **no shutdown** on the controller.

- CSCug97639

  Symptom: IPv4 VRF ping fails when disabling IPv6 unicast-routing globally on the router.

  Conditions: This issue occurs when IPv6 unicast-routing is disabled.

  Workaround: Enable IPv6 unicast-routing

- CSCuh06123

  Symptom: Incorrect quality level (QL) mapping between the clock class and quality level on the PTP master.

  Conditions: This issue is seen when QL value is configured before configuring the PTP master.

  Workaround: Reconfigure the QL values or reload the router.

- CSCuh18073

  Symptom: In a domain with 2 BGP exit points acting in Active or Repair mode, the traffic exits the domain through Repair Path BGP PE instead of exiting through Active Path BGP PE.

  Conditions: This issue exists when the environment has 2 BGP exit points.

  Workaround: There is no workaround.

- CSCuh22045

  Symptom: Small MTU size is not fragmented on the OC-3 IM.

  Conditions: This issue occurs after a reload and SSO is performed.

  Workaround: Unconfigure and configure the IM.

- CSCuh46103

  Symptom: The BDI statistics do not get incremented on the router.

  Conditions: This issue occurs when the ingress and egress statistics are displayed using the show int erface bdi or show interface bdi stats command.

  Workaround: Use **show platform hardware pp active interface statistics bdi** command.

- CSCuh81658

  Symptom: PTP packets are being treated as default packets even though QOS policy is configured

  Conditions: Thi issue occurs afer CPU generated PTP packets do not reach egress QoS with high priority label (15 or 126) and hence does not hit the corresponding default port entries or even the EFP policy's control entries matching these labels.

  Workaround: There is no workaround.

- CSCuh93765

  Symptom: The interface goes down reporting loss of frame alarm.

  Conditions: This issue occurs on performing **shutdown** followed by a **no shutdown** on the PE and CE.

  Workaround: Perform an OIR on CE side.

- CSCui22637

Symptom: Crash observed on the router after unconfiguring 1000 psuedowires.

Conditions: This issue occurs after unconfiguring 1000 psuedowires at a stretch.

Workaround: There is no workaround.

- CSCui30240

  Symptom: 'SPA is not initialized' messages are seen on bootup.

  Conditions: This message is seen post bootup as well during **shutdown** command followed by a **no shutdown** command is issued on the controller. This issue occurs on remote PE reload.

  Workaround: Disable console logging.

- CSCui34041

  Symptom: Traffic is not flowing for one of the prefix.

  Conditions: This issue occurs when the MAX MPLS label of that template is assigned to that prefix.

  Workaround: Disable and enable that prefix.

- CSCui34989

  Symptom: OC-3 IM IOMD crash is seen post SSO.

  Conditions: This issue occura after SSO is performed.

  Workaround: There is no workaround.

- CSCui47776

  Symptom: Virtual circuit receive counters do not increment after SSO is performed.

  Conditions: This issue occurs when 1000 VCs are configured and SSO is performed.

  Workaround: There is no workaround.

- CSCui52938

  Symptom: Layer 3 interface adjacency is incomplete.

  Conditions: This issue occurs after the RSP is removed from the router.

  Workaround: There is no workaround.

- CSCui55567

  Symptom: Traffic convergence for OC-3 IM with TDM features such as serial, MLPPP or POS is high after RSP SSO.

  Conditions: This issue occurs after SSO is performed.

  Workaround: There is no workaround.

- CSCui75901

  Symptom: Sync packets are not sent at a regular interval by the router and inter-packet gap is not within the standard range.

  Conditions: This issue occurs under normal conditions.

  Workaround: There is no workaround.

- CSCui97872

  Symptom: The controller remains in disabled state after enabling the license.

  Conditions: This issue occurs on performing IM OIR or framing.

  Workaround: Disable the license and enable it.

- CSCuj06140

  Symptom: SPAN captured packet has wrong destination MAC addresss.

  Conditions: This issue is seen when MPLS-TP BFD packet is captured.

  Workaround: There is no workaround.

- CSCuj07507

  Symptom: High convergence for downstream traffic observed on the router.

  Conditions: This issue occurs when VPLS VFI's controlled by g.8032 open ring with a large scale of about 500VC's and 10000 MAC address (40 per BD).

  Workaround: Use a lower MAC address scale.

- CSCuj46477

  Symptom: Layer 2 multicast traffic stops on VPLS VCs and starts flowing back on the ingress EFP.

  Conditions: This issue occurs when one of the VPLS VC goes down.

  Workaround: Traffic resumes after the VC comes up.

- CSCuj55599

  Symptom: ARP request for HSRP VRRP MAC (VMAC) is not punted to CPU.

  Conditions: This issue occurs whiel sending unicast ARP packets on the router.

  Workaround: There is no workaround.

- CSCuj76162

  Symptom: The input error counter constantly increases in **show platform infrastructure lsmpi** command.

  Conditions: This problem occurs when the synchronous mode is configured on the interface of router.

  Workaround: There is no workaround.

- CSCul14925

  Symptom: The following message displays on the console:

  %PMAN-3-PROCHOLDDOWN: SIP1: pman.sh: The process iomd has been helddown (rc 143)

  Conditions: When you perform a hard interface module (IM) online insertion and removal (OIR), IM pull out, or soft IM OIR and IOMD is gracefully terminated from the kernel.

  Workaround: There is no workaround. There is no service impact.