Arista Networks EOS 4.24.2.9F Release Notes

Version: 1.0

04 November 2021

Table of Contents

DCS-7170 Series

- DCS-7170 Series

CCS-720XP Series

DCS-7160, DCS-7170, DCS-7280R and DCS-7280R2 Series

7368, DCS-7300X, DCS-7500R and DCS-7800 Series

CCS-720XP Series

DCS-7020, DCS-7280R, DCS-7280R2, DCS-7280R3, DCS-7500R, DCS-7500R2, DCS-7500R3 and DCS-7800R3 Series

- DCS-7280R and DCS-7500R Series
- DCS-7280R2 and DCS-7500R2 Series
- DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series
- DCS-7020 Series
- DCS-7500R3 and DCS-7800R3 Series
- DCS-7020R, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series

DCS-7280R and DCS-7280R2 Series

7300X3, 7320X, 7368, CCS-720XP, DCS-7010, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7060X4, DCS-7250X, DCS-7260X, DCS-7260X3 and DCS-7300X Series

- DCS-7010 Series
- 7320X, DCS-7060X and DCS-7260X Series
- DCS-7260X3 Series
- 7368 and DCS-7060X4 Series
- DCS-7050X, DCS-7250X and DCS-7300X Series
- DCS-7050X2 Series
- CCS-720XP Series
- DCS-7050X3 Series

Transceiver Series

7300X3, CCS-720XP and DCS-7050X3 Series

DCS-7160 Series

Limitations and Restrictions in 4.24.2.9F

Accelerated System Update

BGP EVPN L2/L3 VXLAN/MPLS

CVX

General

Layer 1

Layer 2

Layer 3

- Multi-agent
- Rib

MLAG

MPLS

Multicast

SwitchApp

vEOS Router / CloudEOS

DCS-7170 Series

- DCS-7170 Series

CCS-720XP Series

DCS-7160, DCS-7170, DCS-7280R and DCS-7280R2 Series

7368, DCS-7300X, DCS-7500R and DCS-7800 Series

CCS-720XP Series

DCS-7020, DCS-7280R, DCS-7280R2, DCS-7280R3, DCS-7500R, DCS-7500R2, DCS-7500R3 and DCS-7800R3 Series

- DCS-7280R and DCS-7500R Series
- DCS-7280R2 and DCS-7500R2 Series
- DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series

DCS-7020 Series

DCS-7020R, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series

DCS-7280R and DCS-7280R2 Series

7300X3, 7320X, 7368, CCS-720XP, DCS-7010, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7060X4, DCS-7250X, DCS-7260X, DCS-7260X3 and DCS-7300X Series

DCS-7010 Series

7320X, DCS-7060X and DCS-7260X Series

DCS-7260X3 Series

7368 and DCS-7060X4 Series

DCS-7050X, DCS-7250X and DCS-7300X Series

DCS-7050X2 Series

Transceiver Series

7300X3, CCS-720XP and DCS-7050X3 Series

DCS-7160 Series

Conditions and Impacts

EOS 4.24.2.9F Release Highlights

New Platforms and Hardware

- None

SNMP MIBs

- SNMPv2, SNMPv3
- RFC 3635 EtherLike-MIB
    - obsoletes RFCs 1650, 2358, 2665
- RFC 3418 SNMPv2-MIB
    - obsoletes RFCs 1450, 1907
- RFC 2863 IF-MIB
    - obsoletes RFCs 1229, 1573, 2233
- RFC 2864 IF-INVERTED-STACK-MIB
- RFC 4292 IP-FORWARD-MIB
    - obsoletes RFC 1354
- ARISTA-SW-IP-FORWARD-MIB
    - IPv4 only
- RFC 4363 Q-BRIDGE-MIB
- RFC 4188 BRIDGE-MIB
- ARISTA-BRIDGE-EXT-MIB
- RFC 4113 UDP-MIB
    - obsoletes RFC 1213
- RFC 4022 TCP-MIB
    - obsoletes RFC 1213
- RFC 4293 IP-MIB
    - obsoletes RFC 1213
- HOST-RESOURCES-MIB
- LLDP-MIB
- LLDP-EXT-DOT1-MIB
- LLDP-EXT-DOT3-MIB
- ENTITY-MIB
- ENTITY-SENSOR-MIB
- ENTITY-STATE-MIB
- RMON-MIB
    - rmonEtherStatsGroup
- RMON2-MIB
    - rmon1EthernetEnhancementGroup
- HC-RMON-MIB
    - etherStatsHighCapacityGroup
- RFC 3636 MAU-MIB
    - ifMauDefaultType and ifMauAutoNegStatus are writeable

- SNMP-TLS-TM-MIB
    - RFC 6353
- SNMP-TSM-MIB
    - RFC 5591
- ARISTA-ACL-MIB
- ARISTA-SNMP-TRANSPORTS-MIB
    - 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- ARISTA-SMI-MIB
    - 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- ARISTA-PRODUCTS-MIB
    - 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- ARISTA-QUEUE-MIB
    - Excluding 7150
- RFC 4273 BGP4-MIB
- RFC 4750 OSPF-MIB
- ARISTA-CONFIG-COPY-MIB
- ARISTA-CONFIG-MAN-MIB
- ARISTA-REDUNDANCY-MIB
    - 7500R, 7500E, 7300X, 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- MSDP-MIB
- PIM-MIB
- IGMP-MIB
- IPMROUTE-STD-MIB
- VRRPV2-MIB
- ARISTA-QOS-MIB
- ARISTA-ENTITY-SENSOR-MIB
- ARISTA-BGP4V2-MIB
- ARISTA-VRF-MIB
- ARISTA-DAEMON-MIB
- ARISTA-IF-MIB
    - 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- ARISTA-MAU-MIB
    - 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- ARISTA-PFC-MIB
    - 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- ARISTA-FIB-STATS-MIB
- ARISTA-GENERAL-MIB
- ARISTA-HARDWARE-UTILIZATION-MIB
- ARISTA-NEXTHOP-GROUP-MIB
- ARISTA-SW-IP-FORWARDING-MIB
- ARISTA-TEST-MIB
- ARISTA-XCVR-DWDM-MIB
- ARISTA-XGS-MIB
- IEEE8021-PFC-MIB
- IEEE8021-SECY-MIB
- IEEE8023-LAG-MIB
- MPLS-LDP-STD-MIB

- NOTIFICATION-LOG-MIB
- OSPF-TRAP-MIB
- OSPFV3-MIB
- PTPBASE-MIB

SNMP Traps

- RFC 2863 IF-MIB
    - linkUp, linkDown
- LLDP-MIB
    - lldpRemTablesChange
- RFC 3418 SNMPv2-MIB
    - coldStart
- NET-SNMP-AGENT-MIB
    - nsNotifyRestart
- ENTITY-MIB
    - entConfigChange
- ENTITY-STATE-MIB
    - entStateOperEnabled, entStateOperDisabled
- OSPF-MIB
    - ospfNbrStateChange, ospfIfConfigError, ospfIfAuthFailure, ospfIfStateChange
- BGP4-MIB
    - bgpEstablished, bgpBackwardTransition
- ARISTA-REDUNDANCY-MIB
    - aristaRedundancySwitchOverNotif only for: 7500R, 7500E, 7300X, 7050X2, 7060X, 7260X,7320X, 7060X2, 7160,7020R
- ARISTA-CONFIG-MAN-MIB
    - aristaConfigManEvent
- SNMPv2-MIB
    - authenticationFailure
- VRRPv2-MIB
    - vrrpTrapNewMaster
- MPLS-LDP-STD-MIB
    - mplsLdpSessionUp, mplsLdpSessionDown
- MSDP-MIB
    - msdpEstablished, msdpBackwardTransition
- PIM-MIB
    - pimNeighborLoss
- ARISTA-BRIDGE-EXT-MIB
    - aristaMacMove, aristaMacLearn, aristaMacAge

Supported Hardware

Fixed System

- DCS-7170-64C
- DCS-7280QRA-C36S-R
- DCS-7050TX-64

- DCS-7170-64C-F
- DCS-7170-64C-R
- DCS-7170-32C
- DCS-7170-32C-F
- DCS-7170-32C-M-F
- DCS-7170-32C-M-R
- DCS-7170-32C-R
- DCS-7170-64C-M-F
- DCS-7170-64C-M-R
- DCS-7170-32CD
- DCS-7170-32CD-F
- DCS-7170-32CD-R
- FAN-7001C
- PWR-1100AC
- PWR-1100AC-F
- PWR-1100AC-R
- PWR-750AC
- PWR-750AC-F
- PWR-750AC-R
- PWR-500-DC
- PWR-500-DC-F
- PWR-500-DC-R
- PWR-500AC
- PWR-500AC-F
- PWR-500AC-R
- PWR-745AC
- PWR-745AC-F
- PWR-745AC-R
- FAN-7010
- PWR-1900-DC
- PWR-1900-DC-F
- PWR-1900-DC-R
- PWR-1900AC
- PWR-1900AC-F
- PWR-1900AC-R
- PWR-747AC
- PWR-747AC-F
- PWR-747AC-R
- FAN-7002H
- FAN-7002H-R
- FAN-7000H-R
- PWR-1600AC
- PWR-1600AC-F
- FAN-7001D
- FAN-7001D-F
- FAN-7001C-F
- PWR-400AC-BLUE
- DCS-7280SR2A-48YC6
- DCS-7280SR2A-48YC6-F
- DCS-7280SR2A-48YC6-M-F
- DCS-7280SR2A-48YC6-M-R
- DCS-7280SR2A-48YC6-R
- DCS-7280SRA-48C6
- DCS-7280SRA-48C6-F
- DCS-7280SRA-48C6-M-F
- DCS-7280SRA-48C6-M-R
- DCS-7280SRA-48C6-R
- DCS-7280TRA-48C6
- DCS-7280TRA-48C6-F
- DCS-7280TRA-48C6-M-F
- DCS-7280TRA-48C6-M-R
- DCS-7280TRA-48C6-R
- DCS-7020TRA-48
- DCS-7020TRA-48-F
- DCS-7020TRA-48-R
- DCS-7280CR2A-60
- DCS-7280CR2A-60-F
- DCS-7280CR2K-60
- DCS-7280CR2K-60-F
- DCS-7280SRAM-48C6
- DCS-7280SRAM-48C6-F
- DCS-7280SRAM-48C6-R
- DCS-7280CR2-60
- DCS-7280CR2-60-F
- DCS-7280CR2A-30
- DCS-7280CR2A-30-F
- DCS-7280CR2K-30
- DCS-7280CR2K-30-F
- DCS-7280QRA-C36S-M-F
- DCS-7280QRA-C36S-M-R
- DCS-7280SR2K-48C6
- DCS-7280SR2K-48C6-M-F
- DCS-7280SR2K-48C6-M-R
- DCS-7020SR-24C2
- DCS-7020SR-24C2-F
- DCS-7020SR-24C2-R
- DCS-7280CR2M-30
- DCS-7280CR2M-30-F
- DCS-7280SRM-40CX2
- DCS-7280SRM-40CX2-F
- DCS-7280SRM-40CX2-R
- DCS-7020SR-32C2-F
- DCS-7020SR-32C2-R
- DCS-7020SRG-24C2
- DCS-7050TX-64-F
- DCS-7050TX-64-R
- DCS-7050TX-64-SSD-F
- DCS-7050TX-64-SSD-R
- DCS-7050TX-72-SSD-F
- DCS-7050TX-72-SSD-R
- DCS-7050TX-96-SSD-F
- DCS-7050TX-96-SSD-R
- DCS-7010T-48
- DCS-7010T-48-F
- DCS-7010T-48-R
- DCS-7050SX-72
- DCS-7050SX-72-F
- DCS-7050SX-72-R
- DCS-7050SX-72-SSD-F
- DCS-7050SX-72-SSD-R
- DCS-7050SX-96
- DCS-7050SX-96-F
- DCS-7050SX-96-R
- DCS-7050SX-96-SSD-F
- DCS-7050SX-96-SSD-R
- DCS-7050TX-128-SSD-F
- DCS-7050TX-128-SSD-R
- DCS-7050TX-72-F
- DCS-7050TX-72-R
- DCS-7050TX-96-F
- DCS-7050TX-96-R
- DCS-7010T-48-DC
- DCS-7010T-48-DC-F
- DCS-7010T-48-DC-R
- DCS-7260QX-64
- DCS-7260QX-64-F
- DCS-7260QX-64-R
- DCS-7260QX-64-SSD-F
- DCS-7260QX-64-SSD-R
- DCS-7050SX-72Q
- DCS-7050SX-72Q-F
- DCS-7050SX-72Q-R
- DCS-7050TX-72Q
- DCS-7050TX-72Q-F
- DCS-7050TX-72Q-R
- DCS-7050QX2-32S
- DCS-7050QX2-32S-F
- DCS-7050QX2-32S-R
- DCS-7050SX2-128
- DCS-7050SX2-128-F
- DCS-7050SX2-128-R

- FAN-7011M
- FAN-7011M-F
- FAN-7011M-R
- PWR-1021-AC-RED
- PWR-511-AC-BLUE
- PWR-511-AC-RED
- PWR-621-AC-RED
- FAN-7001C-R
- PWR-400AC-RED
- FAN-7001DH
- FAN-7001DH-F
- PWR-1611-AC-RED
- PWR-1611-DC-RED
- FAN-7011H
- FAN-7011H-F
- FAN-7011H-R
- PWR-511-DC-BLUE
- PWR-511-DC-RED
- PWR-1511-AC-BLUE
- PWR-1511-AC-RED
- PWR-1511-DC-BLUE
- PWR-1511-DC-RED
- PWR-1011-AC-RED
- PWR-721-DC-RED
- PWR-621-AC-BLUE
- FAN-7012H-RED
- PWR-1011-AC-BLUE
- PWR-1011-DC-BLUE
- PWR-1011-DC-RED
- PWR-2411-AC-RED
- PWR-2411-DC-RED
- FAN-7012H-BLUE
- FAN-7012M-BLUE
- FAN-7012M-RED
- FAN-7000
- FAN-7000-F
- FAN-7000-R
- PWR-460AC
- PWR-460AC-F
- PWR-460AC-R
- PWR-460DC
- PWR-460DC-F
- PWR-460DC-R
- DCS-7280TR-48C6
- DCS-7280QRA-C36S
- DCS-7020SR-32C2
- DCS-7280CR-48
- DCS-7020SRG-24C2-F
- DCS-7020SRG-24C2-R
- DCS-7280CR3-32P4
- DCS-7280CR3-32P4-F
- DCS-7280CR3-32P4-M-F
- DCS-7280CR3-32P4-M-R
- DCS-7280CR3-32P4-R
- DCS-7280CR3K-32P4
- DCS-7280CR3K-32P4-F
- DCS-7280CR3K-32P4-R
- DCS-7280CR3-32D4
- DCS-7280CR3-32D4-F
- DCS-7280CR3-32D4-M-F
- DCS-7280CR3-32D4-M-R
- DCS-7280CR3-32D4-R
- DCS-7280CR3K-32D4
- DCS-7280CR3K-32D4-F
- DCS-7280CR3K-32D4-R
- DCS-7280PR3-24
- DCS-7280PR3-24-F
- DCS-7280PR3-24-M-F
- DCS-7280PR3K-24
- DCS-7280PR3K-24-F
- DCS-7280DR3-24
- DCS-7280DR3-24-F
- DCS-7280DR3-24-M-F
- DCS-7280CR3-96
- DCS-7280CR3-96-F
- DCS-7280CR3K-96
- DCS-7280CR3K-96-F
- DCS-7280CR3MK-32P4
- DCS-7280CR3MK-32P4-F
- DCS-7280CR3MK-32P4-R
- DCS-7280DR3K-24
- DCS-7280DR3K-24-F
- DCS-7280CR3MK-32D4
- DCS-7280CR3MK-32D4-F
- DCS-7280CR3MK-32D4-R
- DCS-7050TX-128
- DCS-7050TX-72
- DCS-7050TX-96
- CCS-720XP-24Y6
- CCS-720XP-48Y6
- DCS-7050SX-128
- DCS-7050SX-128-F
- DCS-7050SX-128-R
- DCS-7050SX-128-SSD-F
- DCS-7050TX2-128
- DCS-7050TX2-128-F
- DCS-7050TX2-128-R
- DCS-7050SX2-72Q
- DCS-7050SX2-72Q-F
- DCS-7050SX2-72Q-R
- DCS-7060CX-32S
- DCS-7060CX-32S-F
- DCS-7060CX-32S-R
- DCS-7060CX2-32S
- DCS-7060CX2-32S-F
- DCS-7060CX2-32S-R
- DCS-7260CX-64
- DCS-7260CX-64-F
- DCS-7260CX-64-R
- DCS-7260CX-64-SSD-F
- DCS-7260CX-64-SSD-R
- DCS-7060SX2-48YC6
- DCS-7060SX2-48YC6-F
- DCS-7060SX2-48YC6-R
- DCS-7260CX3-64
- DCS-7260CX3-64-F
- DCS-7260CX3-64-R
- DCS-7050CX3-32S
- DCS-7050CX3-32S-F
- DCS-7050CX3-32S-R
- DCS-7050SX3-48YC12
- DCS-7050SX3-48YC12-F
- CCS-720XP-24ZY4
- CCS-720XP-24ZY4-F
- CCS-720XP-48ZC2
- CCS-720XP-48ZC2-F
- DCS-7050SX3-48YC8
- DCS-7050SX3-48YC8-F
- DCS-7050SX3-48YC8-R
- DCS-7260CX3-64E
- DCS-7260CX3-64E-F
- DCS-7260CX3-64E-R
- DCS-7060DX4-32
- DCS-7060DX4-32-F
- DCS-7060PX4-32
- DCS-7060PX4-32-F
- CCS-720XP-24Y6-F
- CCS-720XP-48Y6-F
- DCS-7050CX3M-32S
- DCS-7050CX3M-32S-F
- DCS-7050CX3M-32S-R

- DCS-7280CR-48-F
- DCS-7280QR-C36
- DCS-7280QR-C36-F
- DCS-7280QR-C36-M-F
- DCS-7280QR-C36-M-R
- DCS-7280QR-C36-R
- DCS-7280SR-48C6
- DCS-7280SR-48C6-F
- DCS-7280SR-48C6-M-F
- DCS-7280SR-48C6-M-R
- DCS-7280SR-48C6-R
- DCS-7280TR-48C6-R
- DCS-7280TR-48C6-F
- DCS-7280TR-48C6-M-F
- DCS-7280TR-48C6-M-R
- DCS-7280QR-C72
- DCS-7280QR-C72-F
- DCS-7280QR-C72-M-F
- DCS-7280QR-C72-M-R
- DCS-7280QR-C72-R
- DCS-7280SR2-48YC6
- DCS-7280SR2-48YC6-F
- DCS-7280SR2-48YC6-M-F
- DCS-7280SR2-48YC6-M-R
- DCS-7280SR2-48YC6-R
- DCS-7020TR-48
- DCS-7020TR-48-F
- DCS-7020TR-48-R
- DCS-7280QRA-C36S-F
- DCS-7050SX-128-SSD-R
- DCS-7250QX-64
- DCS-7250QX-64-F
- DCS-7250QX-64-R
- DCS-7250QX-64-SSD-F
- DCS-7250QX-64-SSD-R
- DCS-7050QX-32
- DCS-7050QX-32-F
- DCS-7050QX-32-R
- DCS-7050QX-32-SSD-F
- DCS-7050QX-32-SSD-R
- DCS-7050QX-32S
- DCS-7050QX-32S-F
- DCS-7050QX-32S-R
- DCS-7050QX-32S-SSD-F
- DCS-7050QX-32S-SSD-R
- DCS-7050SX-64
- DCS-7050SX-64-F
- DCS-7050SX-64-R
- DCS-7050SX-64-SSD-F
- DCS-7050SX-64-SSD-R
- DCS-7050TX-128-F
- DCS-7050TX-128-R
- DCS-7050TX-48
- DCS-7050TX-48-F
- DCS-7050TX-48-R
- DCS-7050TX-48-SSD-F
- DCS-7050TX-48-SSD-R
- CCS-720XP-24Y6-R
- CCS-720XP-48Y6-R
- DCS-7050SX3-48C8
- DCS-7050SX3-48C8-F
- DCS-7050SX3-48C8-R
- DCS-7050TX3-48C8
- DCS-7050TX3-48C8-F
- DCS-7050TX3-48C8-R
- CCS-720XP-96ZC2
- CCS-720XP-96ZC2-F
- DCS-7050SX3-96YC8
- DCS-7050SX3-96YC8-F
- DCS-7050SX3-96YC8-R
- DCS-7160-32CQ
- DCS-7160-32CQ-F
- DCS-7160-32CQ-R
- DCS-7160-48YC6
- DCS-7160-48YC6-F
- DCS-7160-48YC6-R
- DCS-7160-48TC6
- DCS-7160-48TC6-F
- DCS-7160-48TC6-R
- FAN-7002
- FAN-7002-F
- FAN-7002-R
- FAN-7002H-F
- FAN-7000H
- FAN-7000H-F

Modular

- FAN-7002
- FAN-7002-F
- FAN-7002-R
- FAN-7002H-F
- FAN-7000H
- FAN-7000H-F
- PWR-3K-AC
- PWR-3K-AC-F
- PWR-3K-AC-R
- PWR-2700-DC
- PWR-2700-DC-F
- PWR-2700-DC-R
- PWR-3K-DC-BLUE
- PWR-3K-DC-RED
- PWR-3KT-AC-BLUE
- 7500RM-36CQ-LC
- 7500R-8CFPX-LC
- 7500R2-18CQ-LC
- 7500R2-36CQ-LC
- 7516R-FM
- DCS-7516-SUP2
- DCS-7516-SUP2-D
- DCS-7516N
- 7500R2A-36CQ-LC
- 7500R2AK-36CQ-LC
- 7500R2AK-48YCQ-LC
- 7500R2M-36CQ-LC
- 7500R2AM-36CQ-LC
- 7500R3-36CQ-LC
- 7504R3-FM
- 7800R3-36D-LC
- DCS-7508
- DCS-7504
- 7300-SUP
- 7300-SUP-D
- 7300X-32Q-LC
- 7300X-64S-LC
- 7300X-64T-LC
- 7304X-FM
- 7308X-FM
- DCS-7304
- DCS-7308
- 7316X-FM
- DCS-7316
- 7320X-32C-LC

- PWR-3KT-AC-RED
- PWR-D1-3041-AC-BLUE
- PWR-2900AC
- DCS-7504N
- DCS-7508N
- DCS-7500-SUP2
- DCS-7500-SUP2-D
- 7500R-36CQ-LC
- 7500R-36Q-LC
- 7500R-48S2CQ-LC
- 7504R-FM
- 7508R-FM
- 7512R-FM
- DCS-7512N
- 7508R3-FM
- 7500R3K-36CQ-LC
- 7500R3-24P-LC
- DCS-7808-CH
- DCS-7804-CH
- 7800R3-36P-LC
- 7800R3-48CQ-LC
- 7800R3-48CQM-LC
- 7800R3K-48CQ-LC
- 7808R3-FM
- DCS-7800-SUP
- DCS-7800-SUP1A
- 7804R3-FM
- 7500R3-24D-LC
- 7324X-FM
- 7328X-FM
- 7300X3-32C-LC
- 7304X3-FM
- 7308X3-FM
- 7300X3-48YC4-LC
- 7368
- 7368-16C
- 7368-SUP
- 7368-SUP-D
- 7368X4-SC
- 7368-4D
- 7368-4P

Transceiver

- 1000BASE-BX10
- 1000BASE-BX10-D
- 1000BASE-BX10-U
- 40GBASE-AOC
- 10GBASE-LRL
- 10GBASE-ZR
- 40GBASE-PLRL4
- 40GBASE-SR4
- 40GBASE-XSR4
- 40GBASE-LR4
- 40GBASE-LRL4
- 40GBASE-PLR4
- CFP2-100GBASE-LR4
- 10GBASE-AOC
- 40GBASE-UNIV
- 100GBASE-CR4
- 100GBASE-LR4
- 100GBASE-LRL4
- 40GBASE-ER4
- 10GBASE-DWDM
- 10GBASE-DWDM-T
- 10GBASE-DWDM-ZR
- CFP2-100GBASE-ER4
- 100GBASE-PSM4
- 100GBASE-SR4
- 40GBASE-SRBD
- 100GBASE-AOC
- CFP2-100GBASE-XSR10
- 100GBASE-CWDM4
- 25GBASE-AOC
- 100GBASE-SRBD
- 100GBASE-SWDM4
- 100GBASE-ERL4
- 100GE-DWDM2
- CFP2-100G-DWDM-DCO
- CFPX-100G-DWDM
- CFPX-200G-DWDM
- 1000BASE-LX
- 1000BASE-SX
- 1000BASE-T
- 10GBASE-CR
- 10GBASE-LR
- 10GBASE-SR
- 10GBASE-SRL
- 100GBASE-XSR4
- 100GBASE-DR
- 10GBASE-ERBD
- 10GBASE-ERBD-D
- 10GBASE-ERBD-U
- 10GBASE-ERLBD
- 10GBASE-ERLBD-D
- 10GBASE-ERLBD-U
- ADPT-O-Q-100G
- AOC-O-O-400G
- CAB-D-2Q-200G
- CAB-D-2Q-400G
- CAB-D-4Q-200G
- CAB-D-4Q-400G
- CAB-D-8S-200G
- CAB-D-D-400G
- CAB-O-4Q-200G
- CAB-O-4Q-400G
- CAB-O-8S-200G
- CAB-O-O-400G
- OSFP-400G-2FR4
- OSFP-400G-LR8
- OSFP-400G-SR8
- QDD-400G-LR8
- 100GBASE-FR
- CAB-Q-2Q-100G
- OSFP-400G-DR4
- AOC-D-D-400G
- 100GBASE-LR
- SFP-10G-T
- ACC-D-4QN-400
- ACC-O-4QN-400
- OSFP-400G-FR4
- OSFP-400G-XDR4
- QDD-400G-DR4
- QDD-400G-FR4
- QDD-400G-SR8
- QDD-400G-XDR4
- 100GBASE-XCWDM4
- SFP-25G-MR-LR
- SFP-25G-MR-XSR
- SFP-25GR-LR
- SFP-25GR-XSR
- 200GBASE-CR4
- 200GBASE-FR4
- 200GBASE-SR4

- 25GBASE-CR
- 25GBASE-LR
- 25GBASE-SR
- CAB-O-2Q-200G
- CAB-O-2Q-400G
- 10GBASE-ER
- 40GBASE-CR4

Reference to MLAG ISSU Upgrade/Downgrade Table

https://www.arista.com/en/support/mlag-portal

Known Software Caveats in 4.24.2.9F

Accelerated System Update

- Performing SSU when /mnt/flash/persist/persistentRestartLog doesn't exist may result in extended traffic outage due to a watchdog reset that can occur. (158117)
- When performing ASU2 on an MLAG setup with VXLAN configuration, ASU2 can result in a fatal error resulting in a cold boot being performed resulting in large traffic loss. (245555)
  Series Affected: DCS-7060X and DCS-7060X2 Series
- SSU with Splunk enabled may result in extended boot times, which could lead to protocol timeouts or switch cold rebooting. (343629)
- When performing SSU on an MLAG setup, SSU can cause peer links on port-channel to flap, resulting in large traffic loss. (405788)
- sFlow may not work properly after ASU.
  Restarting SandFap agent after ASU will fix the issue. (490542)
  SKUs Affected: DCS-7280SR-48C6-F, DCS-7280SR-48C6-M-F, DCS-7280SR-48C6-M-R, DCS-7280SR-48C6-R, DCS-7280TR-48C6-F, DCS-7280TR-48C6-M-F, DCS-7280TR-48C6-M-R and DCS-7280TR-48C6-R

BGP EVPN L2/L3 VXLAN/MPLS

- BGP agent may crash when multiple vlans are removed from EVPN MAC VRF simultaneously. (481203)
- In a EVPN VXLAN deployment, the BGP agent may restart when removing an Ethernet Segment Identifier associated with a large number of VLANs.

  This is seen at a scale of 250 VLANs. (513122)
- A policy change (such as changing the color extended communities) which causes an L2 EVPN MAC-IP or IMET route to resolve over a different SR-TE policy or tunnel may cause a brief traffic loss. (521090)
- Vxlan agent may produce unexpected dynamic VLAN to VNI bindings when Vxlan is configured with 'hardware forwarding id' feature. (523796)
- A remote VTEP reached through unnumbered BGP over IPv6 will be incorrectly displayed as a configuration error with "FAIL" state due to "No route" (525842)

- Some MAC addresses may get blacklisted when the BGP agent is restarted on a multihomed peer. The workaround is to clear the blacklist using the "clear bgp evpn host-flap" command. (538177)

- In a EVPN MLAG IRB deployment, reloading the the MLAG primary may trigger the lost of some dynamic VLAN allocated for certain VRF to VNI mappings on the secondary.

  The workaround is to restart the VXLAN agent. (548097)

- In an EVPN network, if a MAC address is advertised by a remote device with a non-zero move count and is subsequently removed as a result of a mass withdraw event (EVPN type 1 auto discovery route withdraw), if that MAC address moves to the local device before the remote device withdraws the corresponding EVPN type 2 MAC/IP route, the local device will fail to advertise its own EVPN MAC/IP route. As a workaround, once the relevant MAC/IP routes are withdrawn from the remote device, clearing and re-learning the affected MAC addresses will cause them to be advertised correctly. (549976)

- In a MLAG EVPN IRB deployment, reloading the MLAG secondary may result in an IP-VRF not have an associated VLAN.

  The workaround is to restart the VXLAN agent. (569663)

- When performing an operation that can cause configuration churn on interfaces with Ethernet Segment configuration (such as a config replace) at high scale, the BGP agent may restart unexpectedly. The issue doesn't repeat after the BGP agent has restarted (unless there is another large configuration churn event at high scale). (576033)

- In an EVPN VXLAN deployment, If an EVPN MAC route advertisement is received when the advertiser is unreachable the MAC route will not be install and it will be remain un-installed when the advertiser become reachable.

  A workaround is to un-configure and re-configure the MAC routes' VLAN to VNI mapping. (578329)

- In an EVPN deployment, ARP entries learned from MAC/IP advertisement routes may remain stale after removing the associate MAC-VRF or changing the BGP AS number.

  The workaround is to restart the BGP agent. (578375)

- In a EVPN VXLAN MLAG IRB deployment, remote ARP entries may be discarded when the MLAG peer link is being established.

  The workaround is to restart the VxlanSwFwd agent. (578471)

- In an EVPN multi-homing deployment, designated forwarder election for a given Ethernet segment and EVPN instance pair is based on the complete set of VLANs within the EVPN instance. This differs from the standard in which only the instance VLANs that are in the Ethernet segment interface's allowed VLAN list are used in the election algorithm. This deviation may cause interoperability issues with other vendors.

  As a workaround, a single VLAN-aware bundle EVPN instance may need to be split into multiple instances, such that for every instance and Ethernet segment either every instance VLAN is in the Ethernet segment interface's allowed VLAN list, or none are. (583126)

- In a Multi-VTEP EVPN VXLAN MLAG IRB deployment, reloading both peers may result in the lost of dynamic VLANs on one or both peers required by VRF to VNI configurations.

  A workaround is to restart the VXLAN agent. (586826)

- When moving a VLAN from one VLAN-aware-bundle to another, MACs associated with the VLAN may fail to program if the VLAN was added to the new bundle before it was removed from the old bundle.

  The workaround is to delete and re-add the VLAN, so the VLAN is added while it is not present on any other bundle. (594211)

- In an EVPN deployment, the VLAN flood list may be deleted when moving a VLAN from one VLAN aware bundle to another MAC-VRF.

  The workaround to correct the flood list is to remove the VLAN from the MAC-VRF and then add it back. (603591)

- In an EVPN VXLAN All-Active Multihoming deployment, the ARP entry of a multi-homed host learned through MAC IP route advertisement can be lost. This issue does not apply to IPv6 neighbor entry for a multi-homed host. The issue does not apply to hosts connected via L2 only (no SVI for the VLAN).

  A workaround is to clear the missing ARP entry on the multi-homed peer that learn it over the data plane and advertised the routes. (608813)

- In an EVPN multi-homing deployment, with multiple interfaces in an Ethernet Segment and a large number of allowed VLANs, the BGP agent may unexpectedly due to a configuration change. The configuration changes that can trigger the restart include but are not limited to 1) updates to the Ethernet Segment Identifier; 2) administratively shutting down or enabling a member interface.

  As a workaround, if a port has a large number of allowed VLANs its configuration should be updated separate from that of other ports. (609100)

Containerized EOS

- ISIS/OSPF/OSPF3 may not function properly in cEOS if the kernel interfaces are prefixed with "eth" (397410)

vEOS Router / CloudEOS

- When deleting and adding VRFs on a single VNI, SFE agent may restart and recover after the restart.
  There is no workaround. (542320)

- When an IPsec connection is established with a primary IP address of an interface and a secondary IP address is configured on an interface and that secondary IP address is used to establish an IPsec connection, the IPsec connection with the secondary IP address doesn't come up.
  The workaround is to restart the IPsec agent. (572808)

- A bug in Google Cloud KVM implementation causes Live Migration performed during a
  maintenance event to reload the vEOS router.

  Until a new KVM instance is deployed the only workaround is to modify /mnt/flash/kernel-params to disable hyperthreading using the nosmt parameter. Please contact Arista for detailed steps to apply the workaround. (579590)

- In certain CloudEOS deployments the VM may be oversubscribed and thus subject to processing delays while sending packets to the CPU. This primarily affects BFD control packets and result in the BFD detecting a link flap.

  One workaround is to increase the interval, min-rx and multiplier to larger values for each affected interface. For example, use the command: "bfd interval 500 min-rx 500 multiplier 5" to increase the timeout to 2.5 seconds in the interface sub-mode. (581475)

- BFD/BGP traffic from tunnel interface to CPU goes to low priority queue Q1 (598644)

- hot-add of an interface into the AWS instance running CloudEOS image causes SFE agent to restart unexpectedly. (617390)

- When SFE agent restarts or device reboots, some DPS paths may incorrectly set the loss rate to 50%. This will impact the load balancing of traffic by not utilizing the paths with 50% loss rate to their real capacity. The same issue may also be seen in the scenario where traffic is stopped while there is already significant amount of traffic loss over DPS paths. Auto correction of this issue may take a while to recover the loss rate back to 0 or normal value.

It can be worked around by flapping the corresponding WAN interfaces on the DPS peers of the problematic paths. (618258)

CVP

Network Provisioning

- OpenConfig configurations involving route targets may be incorrectly ignored. (528374)
- ISIS auth config (at global and interface levels) is lost when any ISIS or interface related config is pushed via GNMI or NetCONF. (543354)

CVX

- If a VmTracer session configures all the available VLANs on the switch, then the switch may errdisable the routed ports by freeing up the internal VLANs. (139294)
- On all switch series configured as a MLAG pair where CVX is used as the VXLAN control plane, on rare occasion after a MAC address move between switches the MAC address can be advertised to the CVX server by two different VTEPS. This can cause packets destined to the MAC address to be blackholed. The workaround is to clear the mac address on both the advertising VTEPS so that the mac address will be relearned properly. (158130)
- The MacroSegmentation Service (MSS), working with L2 transparent firewalls, requires the firewall interface be statically identified on CVX via configuration commands (as opposed to using LLDP to detect them dynamically). This prevents issues such as traffic loss in the event that a member port of a aggregated link goes down. (275384)
- Macro-segmentation Service (MSS) might stop intercepting traffic when the last member of the Near service LAG goes down.

  To work around this failure, use the interface mapping from the MSS dynamic device-set configuration to statically map service device interfaces to their corresponding switch port channels. (275656)
- When a security policy on a CheckPoint firewall includes unsupported services, the Macro-Segmentation Service (MSS) intercepts traffic for all services for the specified end-points in the policy. (433067)
- The OpenStack agent may use the wrong region's endpoints for name resolution in multi-region deployments

  A workaround when using CVX to manage only a single region is to redirect

queries to the correct endpoint with 'ip host <wrong endpoint> <correct endpoint ip>'. (503014)

- In a Macro-Segmentation Service (MSS) deployment, a firewall REST API providing a malformed response may cause enforced policy to be withdrawn and re-applied. (512505)
- When 'client state preserve' feature is configured on CVX, state of the primary switch of an MLAG VTEP will not be preserved upon disconnection. If the primary switch did not reboot and disconnected from CVX due to network faults, it may cause disruption of VXLAN control plane leading to VXLAN traffic loss.

  As a workaround, reboot the MLAG primary switch. (533925)
- In a Macro-Segmentation Service (MSS) deployment with Panorama, uncommitted changes to the list of managed devices may be used by MSS to program rules on the switches. (536412)
- When the Policy Control Service is enabled on CVX, under certain circumstances such as re-numbering IP on a host connected to a tagged port, the groups received from NSX controller may not be resolved into IP addresses. This may result in incorrect programming of ACLs on the switches.

  Workaround is to disable and re-enable 'service pcs' on CVX. (538537)
- After a CVX failover the NetworkTopologyAggregator agent may restart.

  A workaround is to trigger another CVX failover. (545008)
- When using Macro Segmentation Service (MSS) with Palo Alto Networks firewall, presence of non-ASCII characters in any field (e.g. policy description) on the firewall might not allow the CVX to retrieve any configuration from it.

  Workaround is to replace non-ASCII characters with their ASCII equivalent if possible. (558655)
- In a VXLAN routing deployment using VCS to distribute MAC and ARP bindings with MSS enabled, if there is an application using a virtual IP address whereby the MAC address bound to the virtual IP address changes as it migrates to behind a different VTEP, then the VTEP may fail to update the ARP entry for the virtual IP to the newer MAC address.

  The workaround is to either disable MSS during the migration, or clear the ARP entries for the virtual IP on the VTEPs prior to migrating the virtual IP. (624581)

General

- When a policy map of type PBR is attached to an interface that is either in down state or a switchport (or both), and if the policy map is too large to fit into available hardware resources, the CLI will not report the error and roll back the configuration. Later, when the interface becomes an operational routed interface, the policy map will not be programmed into hardware. However, "show policy-map type pbr" shows the policy applied to the interface.

  To fix the discrepancy, remove extra rules from the policy map to make it fit into the hardware. (89931)

- OpenFlow Flows may not be programmed in the right priority order after changing OpenFlow Table Profile config to "auto" mode. (118767)
  SKUs Affected: DCS-7260CX3-64, DCS-7260CX3-64-F, DCS-7260CX3-64-R, DCS-7260CX3-64E-F and DCS-7260CX3-64E-R

- While running a combination of both UDP and TCP traffic (e.g. BFD and BGP), a race
condition may lead to a kernel panic due to reusing previously freed memory. (131245)

- The OpenFlow agent fails to return counters associated with a flow, when queried by the OpenFlow controller using protocol version 1.0 (132812)

- On switches using the tg3 driver for the management interface a kernel panic can happen resulting in a switch reload. (136944)
  Series Affected: 7368 Series
  SKUs Affected: DCS-7010T-48-DC-F, DCS-7010T-48-DC-R, DCS-7010T-48-F, DCS-7010T-48-R, DCS-7020SR-24C2-F, DCS-7020SR-24C2-R, DCS-7020SR-32C2-F, DCS-7020TR-48-F, DCS-7020TR-48-R, DCS-7020TRA-48-F, DCS-7020TRA-48-R, DCS-7050CX3-32S-F, DCS-7050CX3-32S-R, DCS-7050QX-32-F, DCS-7050QX-32-R, DCS-7050QX-32-SSD-F, DCS-7050QX-32-SSD-R, DCS-7050QX-32S-F, DCS-7050QX-32S-R, DCS-7050QX-32S-SSD-F, DCS-7050QX-32S-SSD-R, DCS-7050QX2-32S-F, DCS-7050QX2-32S-R, DCS-7050SX-64-F, DCS-7050SX-64-R, DCS-7050SX-64-SSD-F, DCS-7050SX-64-SSD-R, DCS-7050SX-72-F, DCS-7050SX-72-R, DCS-7050SX-72-SSD-F, DCS-7050SX-72-SSD-R, DCS-7050SX-72Q-F, DCS-7050SX-72Q-R, DCS-7050SX-96-F, DCS-7050SX-96-R, DCS-7050SX-96-SSD-F, DCS-7050SX-96-SSD-R, DCS-7050SX2-128-F, DCS-7050SX2-128-R, DCS-7050SX2-72Q-F, DCS-7050SX2-72Q-R, DCS-7050SX3-48YC12-F, DCS-7050TX-48-F, DCS-7050TX-48-R, DCS-7050TX-48-SSD-F, DCS-7050TX-48-SSD-R, DCS-7050TX-64-F, DCS-7050TX-64-R, DCS-7050TX-64-SSD-F, DCS-7050TX-64-SSD-R, DCS-7050TX-72-F, DCS-7050TX-72-R, DCS-7050TX-72-SSD-F, DCS-7050TX-72-SSD-R, DCS-7050TX-72Q-F, DCS-7050TX-72Q-R, DCS-7050TX-96-F, DCS-7050TX-96-R, DCS-7050TX-96-SSD-F, DCS-7050TX-96-SSD-R, DCS-7050TX2-128-F, DCS-7050TX2-128-R, DCS-7060CX-32S-F, DCS-7060CX-32S-R, DCS-7060CX2-32S-F, DCS-7060CX2-32S-R, DCS-7060SX2-48YC6-F,

DCS-7060SX2-48YC6-R, DCS-7160-32CQ-F, DCS-7160-32CQ-R, DCS-7170-32C-F, DCS-7170-32C-M-F, DCS-7170-32C-M-R, DCS-7170-32C-R, DCS-7170-32CD-F, DCS-7170-32CD-R, DCS-7170-64C-F, DCS-7170-64C-M-F, DCS-7170-64C-M-R, DCS-7170-64C-R, DCS-7260CX3-64-F, DCS-7260CX3-64-R, DCS-7280CR2A-30-F, DCS-7280CR2K-30-F, DCS-7280CR2M-30-F, DCS-7280QR-C36-F, DCS-7280QR-C36-M-F, DCS-7280QR-C36-M-R, DCS-7280QR-C36-R, DCS-7280QRA-C36S-F, DCS-7280QRA-C36S-M-F, DCS-7280QRA-C36S-M-R, DCS-7280QRA-C36S-R, DCS-7280SR-48C6-F, DCS-7280SR-48C6-M-F, DCS-7280SR-48C6-M-R, DCS-7280SR-48C6-R, DCS-7280SR2-48YC6-F, DCS-7280SR2-48YC6-M-F, DCS-7280SR2-48YC6-M-R, DCS-7280SR2-48YC6-R, DCS-7280SR2A-48YC6-F, DCS-7280SR2A-48YC6-M-F, DCS-7280SR2A-48YC6-M-R, DCS-7280SR2A-48YC6-R, DCS-7280SR2K-48C6-M-F, DCS-7280SR2K-48C6-M-R, DCS-7280SRA-48C6-F, DCS-7280SRA-48C6-M-F, DCS-7280SRA-48C6-M-R, DCS-7280SRA-48C6-R, DCS-7280SRAM-48C6-F, DCS-7280SRAM-48C6-R, DCS-7280SRM-40CX2-F, DCS-7280SRM-40CX2-R, DCS-7280TR-48C6-F, DCS-7280TR-48C6-M-F, DCS-7280TR-48C6-M-R, DCS-7280TR-48C6-R, DCS-7280TRA-48C6-F, DCS-7280TRA-48C6-M-F, DCS-7280TRA-48C6-M-R, DCS-7280TRA-48C6-R, DCS-7304, DCS-7308, DCS-7504N, DCS-7508N, DCS-7512N and DCS-7516N

- When configuration of a service-policy of type pdp on an interface fails due to lack of hardware resources, the interface may not be protected by any PDP policy. The workaround is to remove the configuration of the PDP service-policy and to configure the PDP service-policy default-pdp-policy on the interface. (216365)

- The CLI command "route-target import auto <ASNumber>" for VLAN VRF does not work and hence should not be used. Alternatively, the suggested configuration is "route-target import auto". In this case the AS Number is picked up from the BGP configuration.

  Example:

```
router bgp 301
   vlan 300
      # This does not work as AS Number for generation of route target is
explicitly
      # configured
      route-target import auto 302

Suggested Usage
router bgp 301
   vlan 300
      # In this case 301 is used as the AS number for generation of route
target
      route-target import auto (255062)
```

- The VM Tracer agent may restart when connected to a VMware vCenter instance with a VMKernel not assigned with an IPv4 address. (258986)
- The MacroSegmentation Service (MSS) feature doesn't work in conjunction with the VARP VTEP IP configuration required for VXLAN routing where a subset of VTEPs are L2 VTEPs. (263532)
- Support for VRRPs in OpenConfig not fully implemented (268736)
- OpenConfig fails because of an invalid type in ISIS with the log message 'expected attribute type nominal.U8, got uint8' (293256)
- When a MLAG peer (configured as a service VTEP for MSS) reloads, MSS re-installs intercept flows which may cause traffic to drop for a short duration. (349254)
- If multiple front-panel ethernet interfaces are configured as reflector interfaces for the same flow of traffic to be reflected, loops can be formed and hosts can flap from one interface to another when the reflector configuration is subsequently changed. The workaround is to only configure one reflector interface to handle traffic reflection. (360869)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- When configuring VXLANs from the EOS CLI, "ip address virtual" is supported and mapped to YANG, but "ip virtual-router address" is not supported. (372193)
- Routing protocols such as OSPF, IS-IS are disabled when VLAN or interface config is changed via gNMI or NETCONF. (401590)
- If a large number of rules are setup on a single 'ip access-list', the OpenConfig agent may use a lot of CPU time and my restart unexpectedly. (407002)
- If the number of PTP vlan's enabled on a switch using 'ptp vlan' command exceeds 65536, PTP agent will become irresponsive and eventually restart. Reducing the VLANs below the limit will avoid getting in this state. (408199)
- When in transparent two-step mode PTP packet sequenceId collision may cause transient jump in offsetFromMaster. Workaround is to use one-step transparent clock mode. (408202)
- DirectFlow 'action output nexthop <ip addr>' ignores TTL of incoming packet and forwards the packet even if the TTL has expired. (417994)
- When an OpenConfig NETCONF client is used to add new classes to policy map, the new classes are added before any previous classes. (451025)

- In rare conditions, the kernel may panic with the message containing "BUG at ../mm/slub.c:3334" (476225)
- Any configured QoS mappings for traffic class to COS and traffic class to DSCP bits are not applied on packets that are reflected via an Interface Reflector that is configured in MAC swap and direction out mode. The source and destination MAC addresses are swapped as expected, but the COS and DSCP bits of the reflected packets are copied unmodified from the original ingressing packet. (476507)
  Series Affected: DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series
- Cli may throw an exception if interface group name or unit name starts with letter 'L'. Workaround is to use any other name not starting with letter 'L'. (486400)
- On system reload, the kernel may crash with the "PANIC: double fault" message. (493516)
- EosSdk agents using a certain combination of Sysdb mount paths may cause the Sysdb agent to restart on connecting to Sysdb. If the agent is configured and stored in startup-config this can cause Sysdb to get stuck in a restart loop. (496371)
- Adding and deleting Nexthop groups via EosSdk APIs, may increase process memory usage over a period of time. (498368)
- Large PTP Offset From Master value fluctuations occur following PTP link failover resulting in disruption to downstream PTP clients. (499397)
- Management interfaces may flap with kernel message "transmit timed out, resetting" and should come back up automatically. On rare occasions an interface will remain down after such flap until the interface PCI device is reset or the system reloaded. (500322)
- The CLI session can close unexpectedly when running a command that internally encounters an IO error. This can happen when running "no shutdown" under daemon mode while the exe is executable but unreadable (e.g., with a permission of 0711). If the command is loaded via a configuration file, partial configuration may be committed. (501541)
- On a device with a high rate of matches against configured STRE policies, the resulting frequent counter update rate can cause OpenConfig to restart unexpectedly. (504297)
- CLI sessions may restart unexpectedly. (506350)
- PTP Sync messages may be buffered and delayed between 6 to 12 seconds. This may cause downstream clients to lose PTP time synchronization. (508551)

- ConnectivityMonitor reports packet loss as 0 instead of 100 in case of a probe error which includes unreachable hosts.
  A workaround for detecting a probe error is to examine the latency statistic which is zero in the case of an error. (512126)

- PTP agent may unexpectedly restart when port-channel links change its status from up to down and vice versa. (519578)

- Flapping port-channel can cause the PTP agent to crash, and bring down all the PTP interfaces. The PTP agent will then restart itself, and all the PTP port will recover and resume normal operation. However, during the the time when PTP is down, the downstream device can lose sync, which cause instability. (519727)

- A customer-provided agent using EosSdk may restart when configuring or modifying an ACL. (524324)

- Applying a Policy-map created through OpenConfig may result in unexpected restart of the Strata-FixedSystem agent (525595)

- Configuring anything on EOS via OpenConfig may fail if BFD is configured. (526372)

- A mis-configuration of the event-handler feature when it uses the on-logging trigger with no regex command will result in a continuous triggering of the handler's action. (528458)

- OpenConfig can experience a memory leak when BGP is accepting dynamic peers. (533842)

- Octa can incorrectly report collection entries as deleted under /Smash eos native paths.

  Restarting Octa will make the incorrectly reported deleted entries appear again, however they or other entries can subsequently be incorrectly reported as deleted again. (537209)

- When a member interface of a PTP-enabled port channel is removed from the port channel, a subsequent speed change on the former member interface may cause the Strata agent to unexpectedly restart. A workaround would be to disable PTP on the port channel before removing the member interface. (540175)
  Series Affected: DCS-7050CX3, DCS-7050SX3 and DCS-7050TX3 Series

- The "arp reply relay" feature does not support a VXLAN domain with L2 VTEPs. (540369)

- In certain cases when a device is reconfigured or an agent restarts unexpectedly, OpenConfig and Octa can stop streaming updates for EOS-native / Smash paths and certain interface counter, BGP and IS-IS paths.

The workaround is to restart OpenConfig or Octa. (542677)

- EOS is not vulnerable to CVE-2020-26116. However, custom agents using the python3 runtime can be vulnerable. http.client in Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9, and 3.8.x before 3.8.5 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request. The fix for this CVE-2020-26116 prevents header injection in http methods. (543494)
- EOS is not vulnerable to CVE-2019-20907. However, custom agents using the python3 runtime can be vulnerable.

  In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation. The fix for CVE-2019-20907 updates the python3 tarfile module to prevent an infinite loop. (543497)
- If an OpenConfig RESTCONF server is configured with an access control list, then the ACL may not take effect. (548311)
- A NETCONF edit-config request for classes in a policy map may cause a change in the order of classes in the same policy map or another one. (550060)
- OpenConfig mixed schema configuration request can fail if the CLI modes send are capable of accepting a "commit" CLI. A workaround is to add the "commit" as part of the request. (554372)
- Modular switch may restart in case of Fabric or Linecard failure. (554503)
- In certain circumstances, when a process takes large amount of memory, it may trigger a kernel panic. (556742)
- BmpAgent, Sflow or BgpCliHelper may abort and restart with the agent log message "DirectRegionHugeMap::remove() i:42 is not region:XXX" (563870)
- Source interface configuration in connectivity monitor is only supported for physical interfaces. (564121)
- In PTP transparent clock mode, a PTP packet updated by the switch may have its VLAN tag stripped when it is forwarded. This can happen if the VLAN-tagged PTP packet ingresses a PTP-enabled VLAN trunk port, egresses a PTP-enabled VLAN trunk port, and there are other PTP-enabled ports configured with a switchport access VLAN. (566037)
- If PTP is configured, performing a configure replace that disables PTP and performs speed changes on interfaces may not disable PTP on those interfaces. A workaround would be to toggle PTP globally or toggle PTP on PTP disabled ports. (569723)

- In PTP boundary mode, configuring P2P delay mechanism on a master PTP port will cause the reported mean path delay to be incorrect. (572766)
- Adding or modifying class-map in a policy-map via OpenConfig may not result in applying the new policy-map in hardware. (573971)
- Adding or modifying Route-map via OpenConfig may not result in applying the new Route-map in hardware. (575325)
- In PTP boundary mode, if the switch is currently slaved to an upstream clock on a port, then PTP state changes on other PTP ports may cause the skew value to not update for a period of time. (575601)
- Configuring "tunnel underlay vrf <vrfName>" before <vrfName> has been applied causes the "tunnel underlay vrf <vrfName> configuration to fail. This error can occur during system startup and config replace operations. The workaround: configure <vrfName> before applying "tunnel underlay vrf <vrfName>". (581461)
- In a VXLAN routing setup using MLAG configuration, there may be excessive UDP (port 51023) traffic observed over the MLAG peer link. This occurs when there is lots of VXLAN ARPs received from remote VTEPs with sender MAC set to virtual MAC. The excessive traffic may result in self-IP queue drops on the receiving MLAG peer, and high CPU utilization by VxlanSwFwd agent on the sending MLAG peer. (583243)
- In a VM Tracer deployment, connecting to a vCenter instance managing an unresponsive ESX host may cause the VM Tracer agent to restart and prevent the processing of CDP and LLDP updates from other ESX hosts. (591593)
- Under a high system load, the PTP agent may intermittently fail to generate packets to downstream PTP devices. There is no known workaround for this issue. (592524)
- In PTP two-step transparent clock mode, delay response packets traversing through the switch may have their correction field incorrectly updated.

  A workaround would be to use PTP one-step transparent clock mode. (592527)
- PORT_ID allocation will fail on systems with more than 4095 interfaces.This includes peer interfaces in an MLAG configuration (593759)
- Resolve issues with incorrect use of AAA APIs. (601875)
- eAPI may skip re-evaluating user credentials when certificate based authentication is used. (606686)
- A gNMI subscriber may not receive all delete messages to an eos_native / Smash path that has had all its elements deleted.

The workaround is for the gNMI subscriber to resynchronize by starting a new Subscribe. (609497)

- A gNMI subscriber may cause Octa to restart unexpectedly if it cancels its subscription shortly after sending a SubscribeRequest. (612780)
- Configuring an ACL on a VLAN interface may lead to a leafref integrity violation in the OpenConfig YANG tree precluding any successful SET operation on the YANG data.
  A workaround is to remove the ACL on the VLAN interface. (614069)
- "reload peer" configured with a delay such as "reload peer in 1 force" results in both supervisors being reloaded after the specified delay. (621572)
- A constant very high rate of events triggering an event handler can cause memory buildup leading to an out-of-memory situation in the system

  Workaround: use the "repeat" event-handler configuration command to limit the rate of event trigger (624314)
- Under periods of high system churn, Octa or OpenConfig agents may restart with a broken pipe panic. The Sysdb agent log will contain a message "Closing connection to Octa ... (AttrLog buffer is full)". The agent should recover when the churn subsides. (627426)
- If ingress sFlow is applied to a mirroring source port which is also used as a nexthop interface for a GRE tunnel used as a destination in any mirror session, then ingress sFlow on that port could stop working.

  A workaround is to disable and then re-enable sFlow on that port; An alternative is to remove the port as a source from its monitor session and then add it back. (629718)
  Series Affected: DCS-7020, DCS-7280CR2, DCS-7280CR3, DCS-7280DR3, DCS-7280PR3, DCS-7280R, DCS-7280R2, DCS-7280R3, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R, DCS-7500R2, DCS-7500R3 and DCS-7800R3 Series

Layer 1

- The forwarding agent may unexpectedly restart after a sequence of speed changes involving speeds of 10G, 25G, 40G, 50G and 100G. (358317)
  Series Affected: DCS-7060X, DCS-7060X2, DCS-7260CX, DCS-7260QX, DCS-7260X and DCS-7260X3 Series
- When a QSFP port is set to 4x25G rate, inserting a 40G QSFP transceiver can trigger a single or continuous forwarding agent restart.
  A workaround is to configure the port for 40G or 4x10G rate before inserting the transceiver. (405185)
  Series Affected: 7300X3, DCS-7050X3 and DCS-7260CX3 Series

- Changing interface speed from forced to auto-negotiated or vice versa may cause the forwarding agent to restart and all interfaces to flap. (491629)
  Series Affected: DCS-7060X4 Series

- Configuring speed, forward error-correction or speed-groups on a large number of interfaces at once may cause the forwarding agent to restart and all interfaces to flap. The workaround is to configure interfaces in smaller batches. (494284)
  Series Affected: 7368 and DCS-7060X4 Series

- Ports configured for 100G without FEC with the CRT50216 PHY may remain down after an AIS or PRBS signal is received.
  A work around is to enable and then disable FEC with 'error-correction encoding reed-solomon' followed by 'no error-correction encoding' (498631)

- Changing interface speed configuration from "speed 50G-1" to "speed auto 50G-2" or "speed 100G-2" to "speed auto 100G-4" causes an unexpected forwarding agent restart. The workaround is to configure "speed 50G-2" or "speed 100G-4" before executing "speed auto 50G-2" or "speed auto 100G-4" accordingly. (500511)
  Series Affected: DCS-7060X4 Series

- MACsec frames shorter than 88-bytes long without SCI and 96-byte MACsec frames with SCI are dropped upon reception. (514526)
  SKUs Affected: 7500R-8CFPX-LC, 7500RM-36CQ-LC, DCS-7050CX3M-32S, DCS-7050CX3M-32S-F and DCS-7050CX3M-32S-R

- Changing interface speed from forced to auto-negotiated or vice versa may cause the forwarding agent to restart and all interfaces to flap. (532747)
  Series Affected: DCS-7060X4 Series

- Changing interface speed from forced to auto-negotiated or vice versa may cause the forwarding agent to restart and all interfaces to flap. (532755)
  Series Affected: DCS-7060X4 Series

- Interfaces drop unencrypted pause or PFC frames while MACsec is enabled. (538882)
  SKUs Affected: 7500R2AM-36CQ-LC, 7500R2M-36CQ-LC, 7800R3-48CQM-LC, DCS-7280CR2M-30, DCS-7280CR2M-30-F, DCS-7280SRAM-48C6, DCS-7280SRAM-48C6-F, DCS-7280SRAM-48C6-R, DCS-7280SRM-40CX2, DCS-7280SRM-40CX2-F and DCS-7280SRM-40CX2-R

- Unencrypted ethernet flow control frames from partner are dropped while MACsec is enabled (539199)
  SKUs Affected: DCS-7280CR3MK-32D4, DCS-7280CR3MK-32D4-F, DCS-7280CR3MK-32D4-R, DCS-7280CR3MK-32P4, DCS-7280CR3MK-32P4-F and DCS-7280CR3MK-32P4-R

- In certain cases like removing the MACsec profile on the key-server, LLPN Exhaustion mechanism is circumvented, causing the B52 agent to restart when rekeying an interface with the maximum transmit PN. (626192)
  SKUs Affected: DCS-7280CR3MK-32P4, DCS-7280CR3MK-32P4-F and DCS-7280CR3MK-32P4-R

Layer 2

- If Ebra agent restarts on a VTEP that is running EVPN control plane with route type 5, then it can result in VxLAN traffic loss. (276063)
- MACsec delay protection feature is not working. (282186)
- When running rapid-PVST at high scales of interfaces and vlans, the device may occasionally not transmit a BPDU, which can lead to a BPDU timeout on the neighbor. (442663)
- Performing an SSO switchover on an MLAG primary peer running Multiple Spanning Tree Protocol may result in STP topology reconverging. (470962)
- Restarting STP agent with a high number of interfaces and vlans in PVST mode may result in STP topology reconverging. (472675)
- VXLAN tunnel termination may be disabled after configuration change, agent restarts or switch reload.

  Workaround is to flap any interface which can cause VXLAN tunnel termination to be reprogrammed correctly. (473246)
- When a port is configured with 'switchport vlan translation <vlan_range> dot1q-tunnel <vlan>' and <vlan> maps to VXLAN VNI, ingress ARP frames with a Dot1Q header setting PCP or DEI bits may cause VxlanSwFwd agent to restart. (524864)
- Re-configuring a member interface from a port-channel configured with "port-channel lacp fallback individual" and currently in fallback individual mode to another port-channel that does not have the fallback configuration can cause the member interface to remain in Bridged forwarding state instead of Data Link. This can potentially cause traffic loop.

  To workaround, un-configure the affected interface from the port-channel and reconfigure it. To avoid this issue while moving an interface from one port-channel to another, un-configure the interface from current port-channel before configuring it into the new port-channel. (525342)
- On a device that's an MLAG or had MLAG configured if egress sFlow is enabled, interfaces can go to blocking with syslog SPANTREE-4-INTERFACE_SELF_LOOPED.

To workaround, disable egress sFlow. (546134)
Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- LACP port-channel member interface(s) may unexpectedly leave the port-channel
due to "partner not in sync" syslog reason without member interface link status
change. The member interface will rejoin the port-channel immediately after. However, the event may cause port-channel interface to flap if there is only one member interface configured in it. (546649)

- On a device that's an MLAG or had MLAG configured in the past and configured with rapid-pvst STP mode, if more VLANs are configured than platform limit, then the StrataVlanTopo agent may continuously restart. Device won't log SPANTREE_TOPOLOGY_LIMIT_EXCEEDED to indicate platform topology limit exceeded.
To workaround, reduce number of VLANs to platform limit specified in Arista product documentation. (548254)

- A Stable Stp agent restart followed by an StpTxRx agent restart can lead to neighbors timing out BPDUs, resulting in an interruption in traffic.

  Changing any STP or interface configuration after the Stp agent restart will avoid this issue. (567341)

- In a VXLAN routing environment using EVPN IRB, when there is a mix of L2 AND L3 VLANs, the ARP and IPv6 ND forwarding traffic can overload the CPU resulting in dropped ARP/ND packets.

  As a workaround, the following configuration adds an ARP/ND proxy deny rule for the default route and reduces the CPU overload, preventing ARP/ND packet drops.

```
!
router l2-vpn
   arp proxy prefix-list disable-default-route-v4
   nd proxy prefix-list disable-default-route-v6
!
ip prefix-list disable-default-route-v4
   seq 10 deny 0.0.0.0/0
!
ipv6 prefix-list disable-default-route-v6
   seq 10 deny ::0/0
!
```

  The above config disables proxy reply for all ARP/ND hosts, and all ARP/ND traffic is forwarded in hardware. The remaining EVPN IRB features (other than proxy reply) continue to function as before. (599556)

- In VXLAN setup using either data plane learning and/or CVX, when anycast gateway is configured with a IPv6 address, then there may be multiple responses to the Network Solicitation for the anycast gateway IP address send from a host. The number of responses will be proportional to the number of anycast gateways in the flooding domain for the VLAN. (609827)
- In a MLAG VXLAN deployment with anycast gateways, ARP synchronization between the MLAG peers may result in packet drops in the CoPP "copp-system-selfip" queue and adversely affect any application traffic over that queue. (616951)

Layer 3

- If a loopback interface is only configured with a link-local IPv6 address, OSPFv3 will not advertise the address. (131369)
- During reload or configuration changes, BFD session may be stuck in init state on one side. Restart Bfd agent to work around the issue. (195545)
- The Ldp agent may restart if configured with a large number of MPLS ECMP routes with many next hops. (273767)
- With scaled VRF config, in the order of 1K VRFs, if the Arp agent restarts, it may fail to come up. (275514)
- In certain scale situations upon a sysdb restart, arp entries can be learned in
  kernel but not show up under 'show arp'. When this happens, the work around is to
  restart the Arp agent. (275749)
- Configuring 'max-metric router-lsa' on an OSPF router may cause summary LSAs to be generated with maximum metric. (276629)
- High rate of ISIS-SR MPLS route churn may cause the Mpls agent to restart. (283149)
- Removing LDP mappings in a large scale LDP configuration may result in LDP neighbor sessions flaps. (283972)
- Auto discovery of multiple IPv6 link-local BGP neighbors over a single interface does not work and will result in only one of the neighbors transitioning to established state. (289875)
- BFD configurations with large numbers of sessions may see BFD session flaps during initial session bringup shortly after boot. (375773)
- When an ARP entry is added while there is a matching, existing virtual IP with a non-/32 subnet, traffic loss may occur because traffic may be flooded instead of forwarded to the CPU.

Workaround is to either use multiagent mode or only configure virtual IPs with a /32 subnet. (402802)

- When graceful restart is enabled under "router isis" and other protocol routes are redistributed into IS-IS then on ASU or SSO, some traffic that is forwarded using redistributed routes might be lost. (413706)
- Removing SVI configuration at scale via a config-replace operation may cause the BFD agent to unexpectedly restart. (414702)
- The MLAG agent may exit unexpectedly after upgrading from 4.22.0 or an older release if the MLAG peer switch is still running the older software version and DHCPv6 prefix delegation routes are being sync'd across the peers. (425810)
- In situations involving a route with a next hop IP getting deleted and added back
  without a next hop IP, static ARP entries falling in the same subnet as the prefix of
  this route may not be correctly added.

  Workaround is to restart the ARP agent. (436002)
- When a series of back-to-back configuration changes are applied to a BFD session, the session may not have the latest configured value. To work around the issue, un-configure and re-configure the BFD session. (458955)
- The output of 'show ip nat sync peer' may incorrectly indicate a connected state, even though an incorrect peer IP address has been configured. (464011)
- DHCP relay agent might exit unexpectedly if several VRFs are continuously deleted and re-created. (471169)
- With 'ipv6 dhcp relay install routes' configured on more than 100 SVIs, DHCP relay agent may exit unexpectedly when a IPv6 DHCP helper address is configured simultaneously on all SVIs. (471338)
- Cspf agent may restart when TI-LFA protection is configured and the number of segments requiring protection is over 2K (481703)
- In EOS, host route computation is facilitated by the Arp agent. In situations with scaled neighbor entries, particularly when all or most of the entries map to the same route, the Arp agent may encounter a heartbeat timeout, leading to the Arp agent restarting. Typically, the Arp agent will run fine after the restart. (484901)
- In EOS, host route computation is facilitated by the Arp agent. In situations where the FIB routing table is at internet scale, particularly if all or most of the routes are tunneled, the Arp agent may encounter a

heartbeat timeout, leading to the Arp agent restarting. Typically, the agent will run fine after restart. (484902)

- In scale situations, if a static ARP entry is added immediately before a route is deleted and re-added, the entry may not be properly added. Workarounds include removing and re-adding the static entry, flapping the interface the entry end up on, or restarting the Arp agent. (486998)
- TI-LFA backup paths will be computed slowly when there are large number of node-segments/anycast-segments/adjacency-segments that are protected. (489097)
- If a configuration change involving deletion of several VLAN interfaces along with anything which causes platform layer 3 agent to restart is applied, then the layer 3 agent may see multiple restarts following the first restart. (492891)
- An LSR which is the penultimate hop in an RSVP LSP may incorrectly report a "bandwidth unavailable" error if the tunnel destination IP is an interface IP that does not match the last hop in the ERO.

  A workaround is to use a loopback interface as tunnel destination or the interface IP that is present in the ERO. (493578)
- If an IP route resolves over ECMP of SR-TE policies containing multiple segment-lists using TI-LFA backup paths, forwarding agents may not properly failover to the backup path. This can happen if link of a primary path goes down and can lead to traffic loss. (497790)
- If a configuration change involving deletion of several VLAN interfaces along with anything which causes platform layer 3 agent to restart is applied, then the layer 3 agent may see multiple restarts following the first restart. (498164)
- After clearing own LSP from IS-IS LSPDB using clear isis database <own LspID>, Isis will fail to export its own LSP information to IGP Topology Database. This can result in CSPF agent to not compute the paths for RSVP and the backup paths for TiLFA. Also setting overload bit after clearing the LSP will cause Isis agent to restart. (498227)
- BFD sessions may continuously flap after a speed change on an interface. A workaround is to restart StrataBfd. (499185)
- When changing the OSPF Router Id, OSPF will not flush its existing self-originated LSAs
  from the routing domain before the new Router Id takes effect (499551)
- Isis agent will restart if an interface has ipv4 unnumbered configuration and ipv6 global address configuration and has enabled ipv4 and ipv6 traffic engineering. (501374)

- If a MPLS L3 EVPN route resolves over a single NexthopGroup tunnel, then the packet may get sent out without the MPLS L3 EVPN encasulation label. The workaround is to issue "ip hardware fib next-hop proxy disabled" command. (501739)

- When a RSVP tunnel A which has bandwidth reserved gets preempted by a higher priority
  tunnel B, sometimes Cspf may not compute an alternate path for A and so the tunnel
  will stay down. One workaround is to change any TE link's attribute like TE metric,
  admin group or SRLG temporarily and revert it back. An unused TE attribute is better,
  because it won't affect already established tunnels. (501974)

- When the IP reachability of the TI-LFA protected link is leaked from one level into another level on the router in level-1 and level-2, then on link down local convergence delay timer is immediately aborted for the protected prefixes. This may cause the traffic loss due to micro loop. (504629)

- Isis agent may restart on a level1-2 IS-IS node when TI-LFA fast-reroute configuration is present and anycast prefix segment is configured on the nodes in different levels such that one node is SR capable and the other node is non SR capable. (508664)

- In high scale, i.e. ~5000 or more tunnels, with a lot of churn of tunnels, creation of new tunnels may fail on LER for several hours. (515508)

- In rare conditions, Cspf agent may unexpectedly restart when a path's configuration is changed by Rsvp agent. (515795)

- Ira agent may restart continuously after an agent-restart or switchover when LDP is configured.

  As a workaround, device should be reloaded. (520036)

- Protocol messages exceeding 1500 bytes are ignored, in particular BUNDLE and SREFRESH messages, which is the case for jumbo frames. The symptom can be dropped LSPs or long convergence times. (521363)

- An RSVP RESV message is immediately sent as a reply to a NACK object, which can lead to a packet storm if an RSVP neighbor incorrectly uses NACK objects as an error reporting mechanism.
  Configuring RSVP with `refresh method explicit` will prevent this issue but disable Refresh Overhead Reduction. (522041)

- If an IPv4 or IPv6 route points to a combination of non-hierarichal next hop as primary next hop and a nexthop group (or nexthop group tunnel) as the backup, the IP route will ignore the primary next hop and forward traffic

toward the backup.
The workaround is to configure 'ip hardware fib next-hop proxy disabled' command. (524238)

- For short-lived TCP connections, NAT may not tear down the address mapping when it should. The workaround is to lower the TCP timeout using the `ip nat translation tcp-timeout` CLI. (526152)
- IP routes and FECs may fail to install in some instances when we recover from a resource overflow scenario. A workaround is to restart the L3 platform agent. (526893)
- After TE router id or IGP router id change of a node on a Rsvp tunnel with BW requirement or a link flap on the tunnel, Rsvp may not correctly update the BW reservation of the tunnel when there is change in BW requirement and/or FRR global reversion may not happen when a link goes down later on the tunnel. (527889)
- If any router on the path expects the "Controlled Load" fragment in the RSVP AdSpec object, then no LSP comes up. (527899)
- On scale setup, with certain network events that cause massive route updates, ARP agent's internal state may go out of sync, leading to the ARP agent repeatedly deleting and adding the same entry to the kernel. This may cause the CPU usage to spike to 100% usage.

  Workaround is to restart the ARP agent. (532708)
- Stateful switchover can cause a small traffic loss because of host routes without ARP resolution. (533234)
- RSVP agent might unexpectedly restart if a bypass is created and deleted quickly. (533402)
- When there are more than 254 RIP enabled interfaces then it may result in restart of the protocol agent if a route needs to be advertised to more than 254 neighbours. (535893)
- When the number of ECMP paths for a RIP route exceeds 600 then the protocol agent may restart. (536038)
- When large number of distribute lists are configured in RIP then it may result in route flaps and the protocol agent CPU utilization can increase significantly. (536500)
- If neither Graceful Restart nor Hold Timer are negotiated for a peer, BMP will not send any Route Monitoring Messages for that particular peer. (539641)

- KernelFib agent may restart on interface flap, if there are a large number of route resolving through that interface (539757)

- When disabling MPLS on an interface in the non-default VRF, it may cause software forwarding or
  control plane generated IP packets for routes which point to tunnels, nexthop-groups or when
  routing from one IP address-family to another (RFC 5549) to route the packet incorrectly.
  This will only affect packets in the default VRF. These packets may end up being routed in
  the non-default VRF.

  Configure an SVI with no autostate configured in the default VRF to work around this issue. (542757)

- RSVP tunnels might not get established or may use non-best paths when IS-IS system ID or OSPF router ID is changed for any node in the IGP network and the best path goes via that node. One workaround is to change the TE router ID also for the same node. (546904)

- KernelFib agent may restart, if EVPN config is toggled in quick succession. (557358)

- On scale setup during certain network events, ARP agent's internal state may go out of sync, leading to ARP agent repeatedly deleting and adding the same entry to the kernel. This may cause the CPU usage to spike to 100% usage.

  Workaround is to restart ARP agent. (559855)

- When using OSPFv3 and encryption or OSPFv2 with SHA encryption, the Rib agent may stop responding and restart unexpectedly. (560294)

- SrTePolicy agent may restart if the top label of the Segment List is resolved over LFIB entry with outgoing label as Explicit Null Label. (561061)

- When TE router ID of one of the two routers which have the same TE router ID is changed to be same as that of a third router, Cspf agent may sometimes restart (565678)

- When 64 areas are configured in OSPFv3, router configuration may not be applied after a system reload. To workaround the issue, configure less than 64 OSPFv3 areas. (570346)

- RSVP tunnels might not get established or may use non-best paths when IS-IS system ID or OSPF router ID of any two neighbouring nodes in the IGP

network is changed back-to-back and the best path goes via that node. (572080)

- KernelFib crashes upon restart when a third party route added through bash or an external agent, is quickly added and deleted before the interface pointed to by the route is UP (574133)
- RSVP tunnels may not get established after changing the OSPF router ID of the designated router (577130)
- If a route received from a BGP peer is leaked from one VRF to another using VrfLeak agent (https://eos.arista.com/eos-4-22-1f/eos-vrfleak-agent/) and the leaked route in the target VRF is again leaked to another VRF using route-target import/export configuration in BGP (https://eos.arista.com/eos-4-21-3f/inter-vrf-local-route-leaking/), the Bgp agent can restart unexpectedly.

  As a workaround, use these mechanism to leak distinct set of routes. If a route has to be leaked across multiple VRFs, use either VrfLeak agent or route-target import/export configuraiton for leaking the route to all the target VRFs. (577257)
- Rib agent or the multiagents (Isis/Ospf) can restart with a large prefix-list configuration (578037)
- A DHCPv6 prefix received with valid lifetime of zero may persist forever in the routing database in the presence of 'ipv6 dhcp relay install routes'. A workaround might be to toggle "ipv6 dhcp relay install routes" command, which deletes all DHCPv6 routes, including the stale ones with negative lifetime. (578276)
- With BFD VXLAN configured, BFD agent restart after a first supervisor failover may result in continuous BFD agent restart.

  There is no workaround once the restart loop starts. Performing another supervisor
  failover before restarting the BFD agent will avoid the restart loop. (586673)
- An IP configured on an interface in a non-default VRF may cause an RSVP LSP to not come up if the same IP appears in that LSP's path for a different router. (591762)
- The OSPF agent may restart when sending a graceful restart LSA on an interface with SHA authentication configured. (593659)
- KernelFib agent may restart when interface flaps lead to a large number of routes (entire routing table) being withdrawn (597557)

- The VxlanSwFwd agent may crash when processing a DAD packet from a host that is destined to a virtual link local address. (602176)
- Isis agent may restart when it receives LSP from any node that advertises SRLG on an unnumbered interface (605131)
- OSPFv3 fails to install routes from intra-area-prefix(NAP) LSAs if the referenced LS ID in the NAP LSA does not match the Link State ID of the RTR LSA (605376)
- In setups with large number of ARP or ND entries in the same subnet, upon a more specific route in that subnet getting removed, the Arp agent may reevaluate all of the ARP or ND entries in that subnet, resulting in high CPU usage in the platform agent.

  Workaround is to split up large connected routes by adding more specific static interface routes to make the subnet that the ARP/ND entries fall under smaller. (606649)
- When auto-cost reference-bandwidth is configured in OSPF and OSPF receives a speed change event with bandwidth value 0 for a port channel interface, OSPF may set the cost of the interface to the default cost (10). This could result in traffic loss since routes may be installed to the port channel that has no bandwidth. (606650)
- ARP requests for NAT pool addresses might fail due to incorrect initialisation.
  As a workaround restart NAT agent to recover from the issue. (610947)
- When there are least two IS-IS adjacencies between the routers and two or more adjacencies have the same associated SRLG value configured. IS-IS agent may restart on one or more nodes when one of the adjacency goes down. (617367)

IPSEC

- Under some circumstances IPsec rekey time may show up as 'N/A'. (561575)

Multi-agent

- If a VRF is deleted while the Bgp agent is in the middle of processing paths in BRIB, it may restart unexpectedly. (209143)
- Performing a stateful switchover in a switch with a large number of VRFs configured, with BGP config in all VRFs and IGPs configured in a large number of VRFs, may cause the system to restart unexpectedly, leading to traffic loss. (376773)

- When sampling packets with the BGP extension enabled, if the address family of the route does not match the address family of the next hop, the sFlow agent can restart unexpectedly.
  When sampling packets with sampled flow tracking, if the address family of the route does not match the address family of the next hop, the SftAgent can restart unexpectedly.

  Use "no sflow extension bgp" to stop the sFlow agent agent from restarting. There is no workaround for sampled flow tracking. (427674)

- ISIS/OSPF/OSPFv3 agents can restart unexpectedly if interface static routes over tunnel interfaces are redistrbuted into them. The workaround is to configure gateway static routes using nexthop IP instead of interface static routes. (450213)

- MplsVpn routes may not get advertised after doing "clear ip bgp *". As a workaround, Bgp agent should be restarted. (472286)

- During BGP graceful restart, 'update wait-for-convergence' behavior is unnecessarily forced for AFI-SAFIs which do not have graceful restart configured (either specifically per AFI-SAFI or globally). (478038)

- Bgp agent may restart unexpectedly when 'bgp always-compare-med' option is configured and large number of competing paths for the same prefix from several neighbors with different MED values are present (482275)

- BGP agent may unexpectedly restart if 'bgp skip rib-install bestpath-selection' is configured.

  Workaround is to disable in-place fec update using 'bgp fec skip in-place update event all' in router bgp config mode (495110)

- If multiple dynamic BGP peers are present in a peer-group and the peer-group has a prefix-list in the configured inbound policy, the enbound policy may not get re-evaluated for all the dynamic peers on modification to the prefix-list.
  "clear ip bgp *" or BGP agent restart can be used to re-evaluate the input policy correctly when this happens. (504936)

- BGP Fallback AS is not supported for dynamic BGP peers (507024)

- At large route scale, the restart of either the Bgp agent or the IpRib agent may cause repeated restart of the IpRib agent (508763)

- When BGP additional-path install is configured, the usage of ECMP FEC resource increases. (514388)

- If a BGP peer (or peer group) description is longer than 255 characters, polling the aristaBgp4V2PeerDescription MIB object may fail. In addition, if BGP traps/notifications are enabled, the Snmp agent will restart whenever

it attempts to send the aristaBgp4V2BackwardTransitionNotification trap.

Workaround: Limit the BGP peer(group) description to 255 characters. (528521)

- "set metric *<number>" action in a route-map allows customer to set multiplicative metric value. This is only supported by the Bgp agent. However, if such a route-map is present, IGP agents (Ospf/Ospf3/Isis/Rip) will continuously restart.

  Workaround: Remove the "set metric *<number>" configuration. (541169)

- A switch configured with MPLS EVPN may proxy reply and not flood a gratuitous ARP announcement message, which may prevent cluster failover migration of a virtual IP to a new server. (541463)

- The configuration 'bgp missing-policy direction out action deny' may be ignored briefly when a route map applied on outbound to a BGP peer is deleted.

  A workaround for this is to remove or replace the route map from the peer without deleting the route map. Once the update has taken effect the route map can be deleted. (554264)

- On a reboot of a modular chassis without linecards, a user configured (non-DEFAULT) VRF exclusively associated with management interfaces has no management connectivity (563022)

- For 6PE session, route refresh requests are sent out for IPv6 Unicast rather than for IPv6 Labeled Unicast. (569595)

- The command 'show bgp neighbor <prefix> history' will cause the Bgp agent to restart unexpectedly if the prefix address given is longer than the length (i.e. 10.1.1.1/24). (573022)

- An IPv6 nexthop may optionally contain an additional link-local IPv6 address. A BGP neighbor sending IPv6 Labeled Unicast NLRI with a nexthop that includes both global and link-local nexthops will be incorrectly marked as malformed, causing IPv6 LU AFI/SAFI to be disabled for that neighbor. (575422)

- In multi-agent mode, when displaying the results of "show ip bgp detail" the output may be corrupted by showing content previously output by the currently running command in place of new content (607255)

- When Class Based Forwarding (CBF) using SR-TE policies in enabled, deactivation of an SR-TE policy that has been used for CBF may cause the IpRib agent to created unneeded drop FECs. This problem can eventually

result in memory exhaustion which causes the IpRib agent to restart. (620077)

- A switch configured with BGP UCMP may fail to advertise a route that rapidly flaps. (627616)

Rib

- In the ribd routing protocol model, prior to EOS 4.21.3F release, the command
  "neighbor <peer|peer-group> send-community extended" (under "router bgp")
  will result in both standard and extended communities being sent
  (in outbound route advertisements) to the corresponding peer.

  Starting with EOS release 4.21.3F this behavior has changed. The command
  "neighbor <peer|peer-group> send-community extended" will result in *only*
  extended communities sent to the peer.

  If the previous behavior is desirable, then the command
  "neighbor <peer|peer-group> send-community" without additional keywords
  can be used. This command will ensure that all applicable community types
  are
  included in outbound route advertisements for the peer.

  This change can be done in any release (running EOS version 4.18.1F or
  newer)
  prior to the upgrade to EOS 4.21.3F (or newer) release.

  EOS 4.21.3F or newer releases allow much more granular control of what
  community
  types (standard, extended, large communities etc.) are included in the
  outbound
  route advertisements. (384629)

- Rib agent may restart with BGP PIC enabled (bgp additional-paths install) under route churn (512675)

- The Rib agent may restart when large number of interfaces go down at the same time and there is a large scale of BGP routes reachable over these interfaces. (549816)

- When the Tunnel agent goes down, stale entries in the tunnel RIB may not be cleaned up upon restart of the agent. (586928)

- RIB agent leaks memory when the color extended community or NextHop attribute changes. With a high scale of BGP routes with color extended community, even without SRTE configured, the RIB agent may restart due to the leak which leads to running out of memory. (615108)

MLAG

- If non-MLAG reload-delay is configured to be lower than the MLAG reload-delay when LACP standby is used, traffic entering the non-MLAG interfaces destined towards hosts on the MLAG interfaces will be lost during the LACP standby period. (83330)
- MLAG ISSU breaks on a switch running a version of EOS < 4.20.5 if it receives ARP entries from the VXLAN Control Service (VCS) while the peer has been upgraded to EOS version >= 4.20.5 (497776)
- In a MLAG VXLAN deployment, the VxlanSwFwd agent may restart when receiving a Gratuitous ARP. (507878)
- When the M-LAGs flap due to missing LACP packets from their partner interfaces and end up in active-partial state while a burst of MAC learning events are being exchanged between the two MLAG peers, then it is possible for the L2 agent to skip programming some of the MAC addresses synced between the two peers.

  The workaround is to flap the M-LAG members on the peer whose MAC table is out of sync. (543878)
- When the address for the MLAG local interface is changed, transmitting and receiving STP BPDUs on the secondary peer may not function correctly, potentially leading to traffic loss. An additional symptom is "waiting for counter update ... timed out" being displayed when running "show spanning-tree
  counters" or other STP show commands that display BPDU counters.

  Workaround is to restart the KernelNetworkInfo agent and then restart the Mlag
  agent. (578635)

MPLS

- Performing SSO, or restarting L3 forwarding agent, on platfroms that support MPLS non stop forwarding, might prevent L3 forwarding agent to warmup.
  The workaround is to perform a hitful restart of L3 forwarding agent. (499349)
- For single hop RSVP tunnels, after FRR failover, the tunnel will oscillate between using the primary and backup LSP's if the primary LSP gets reestablished. (515431)
- MPLS agent might restart due to route churn in FIB containing large number of routes. (526406)

- If MPLS agent restarts when LFIB contains BGU-LU MPLS routes that resolve over ISIS-SR tunnels, the mentioned LFIB routes might not be programmed after restart.

  The workaround is to configure 'fib sharing igp tunnel disabled' command under segment-routing CLI model. (529085)

- Excessive toggling of the 'mpls ip' or 'ip routing' commands may cause the LDP label range to be exhausted.

  Wait for the LDP agent to shutdown after disabling 'mpls ip' before reenabling it to ensure the LDP labels are released. (539317)

- The "configure replace" command causes LDP sessions to be cleared when they were previously cleared using the "clear mpls ldp neighbor". The cleared sessions will immediately recover. (549437)

Multicast

- In a VLAN that only has an IGMP proxy querier(0.0.0.0) present, IGMP snooping does not start flooding traffic in the VLAN when the querier disappears. (258931)

- An S,G route may not properly cleanup previously sent S,G joins. This would prevent S,Gs from being deleted in the upstream router. A work around is to flap the interface in which the join is sent on. (291756)

- If large number of IGMP reports are received in a very short interval, some of them might get dropped resulting in the multicast route not being created. The routes will be re-learnt on the subsequent query interval. If "show cpu counters queue" shows consistent drops under "CoppSystemIgmp", consider increasing the bandwidth for this Copp class. (356675)

- Fast reload fails when multicast is configured on a non-default VRF that is not PIM enabled. The default VRF is always PIM enabled, but a non-default VRF is PIM enabled when it contains at least one PIM interface. Workaround is to enable a PIM interface on each non-default VRF. (398256)

- In an environment with a very large number of MSDP peers, during cleanup the MSDP Agent may unexpectedly restart. (418190)

- Deletion of PrefixIntfSm may cause unexpected restart of the corresponding Mroute agent (471017)

- High CPU utilization might be observed for the forwarding agent when PIM Bidir routes are present. (479119)

- If MLD Snooping is configured, IPv6 multicast packets may not be bridged as expected in a PIM SM or PIM SSM non DR VLAN. (493226)

Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- At switch restart, if PIM BSR configuration exists, PimBsr might crash and could potentially affect existing traffic. (495416)
- BessMgr agent could restart unexpectedly when resolving a large number of unresolved packets at once. (495863)
- Removing router pim bsr also remove router pim sparse mode configuration. Workaround is to just remove specific configuration under router pim bsr mode. (516188)
- If the SandMcast agent restarts while IPv6 multicast routes are programmed, the routes may become incorrectly programmed.
  The programming of the IPv6 multicast routes can be corrected by toggling IPv6 multicast routing off and back on. (519865)
  Series Affected: DCS-7020, DCS-7280CR2, DCS-7280CR3, DCS-7280DR3, DCS-7280PR3, DCS-7280R, DCS-7280R2, DCS-7280R3, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R, DCS-7500R2, DCS-7500R3 and DCS-7800R3 Series
- Using "software-forwarding sfe" for software forwarding of multicast packets does not work on x86_64 version of EOS. (537616)
- Forwarding agent might unexpectedly restart or use incorrect RPF setting during unicast route churn. (539478)
- On devices running PIM, on system boot up, might suffer loss or slower re-convergence of multicast traffic flows. (570930)
- On devices connected to multicast receivers that are part of a MLAG pair, restart of IgmpSnooping/Mlag agent may result to more IgmpSnooping restarts. This state has no impact on forwarding behavior of the box.

  Workarounds: Reload the device (574602)
- Configuring "ip igmp host-proxy <ACL-NAME>" where the access list has a large multicast group prefix length may cause the IgmpHostProxy to be repeatedly restart resulting in traffic loss.
  Use smaller prefix lengths to work around the problem. (586865)
- When an interface is a (*,G) assert loser, traffic duplication might be present until the assert winner sends the next periodic assert of around 3 minutes. (587719)
- The PimBidirDf agent could continuously send DF winners when multiple RPs are configured and one RP is deleted. This may cause high CPU in the PimBidirDf agent. Workaround is to restart the PimBidirDf agent. (603791)

- Periodic PIM assert messages might be sent continuously when the number of winner
  asserts per interval takes more than 0.1 seconds. There is no workaround. (613310)

vEOS Router / CloudEOS

- The OpenFlow agent fails to handle packet-in messages (145001)
- When several IPsec tunnels are up and traffic is passing through them, removal and addition of a IPsec license may cause the the Ipsec agent to restart.

  The workaround is to shutdown all the interfaces before the IPsec license is removed and reapplied and then do a "no shutdown" on the tunnel interfaces. (248213)
- A reboot due to a kernel panic can happen during first 10 minutes of vEOS bootup on Microsoft Azure. The kernel panic occurs because of a task blocking without being scheduled for more than 300 seconds in "D" state. (249618)
- Interface may be allowed to be configured with un-supported speed of NIC using "speed <speed>", which will cause an unexpected PhyEthtool agent restart. Do not use "speed <speed>" command to configure interface speed that NIC does not support. (264395)
- When running vEOS devices in Sfe mode with interfaces having an MTU of 9214, users may encounter a scenario where not all routes are propagated through the network. The workaround is to have interfaces use an MTU of 9202 or less. (289886)
- On vEOS Router in Sfe/DPDK mode with many GRE/IPSec tunnels, changes to configuration may cause a long time to be applied to the datapath. (349552)
- When loading a vEOS instance in an Azure cloud, it is possible for the device to experience a kernel panic just after bootup, causing the device to reboot a second time. (354411)
- In an EVPN IRB deployment on vEOS, changing the VXLAN source-interface interface may result in EVPN ip-prefix routes not getting installed into one or more VRFs for one or more remote VTEPs. (369816)
- When multiple IPSec connections are created, some with AES encryption and some with NULL encryption and NULL authentication, bessd will crash when decrypting the IPsec packets encrypted with NULL encryption and NULL authentication. (378590)
- CloudEOS supports upto 600K BGP routes with 8G of system memory; If 800K BGP routes are programmed, out-of-memory condition will kill random

processes.

Out-of-memory issue can be mitigated by increasing the system RAM to 12G to program 800K BGP routes. (478214)

- When CloudEOS is deployed in Sfe mode on the Azure platform, the agent crashes if
only synthetic NICs are attached and no SRIOV NICs are attached. (483538)
- When CloudEOS is deployed on the AWS platform in Sfe mode, the Sfe agent crashes. (487773)
- If IPv6 or multicast packets are sent to vEOS on two or more interfaces vEOS forwarding engine can crash. Disable IPv6 and mcast configuration on the interfaces of the neigboring routers connected to vEOS. (497553)
- DPS (dynamic path selection) using Ipsec connections may become corrupted in the event of a Sfe agent restart.

  The workaround is to administratively disable and enable the Vxlan1 interface.
  Run "shutdown" then "no shutdown" on the Vxlan1 interface. (503017)
- An improperly formated TCP MSS option can trigger a Sfe dataplane restart. (504565)
- When the Sfe data plane flow cache has reached capacity, IpSec packets which bypass
the flow cache can trigger a data plane restart. (507937)
- Reusing a VNI previously used by VRF-A on VRF-B will affect traffic on VRF-A.

  The workaround is to restart the software forwarding engine (Sfe) agent. (523066)
- The SFE agent may fail to process new flows or restart when closed or reset TCP
sessions are removed from the system. There is no available workaround. (533647)
- Changing the mapping of Vrf to VNI (VXLAN Network Identifier) twice will cause the software forwarding engine (Sfe) agent to restart. There will be a brief moment of traffic loss which will recover eventually. (539064)
- When DPS feture is configured, there is a race condition with a transit router configuration that may lead to an unexpected restart of the Sfe agent. There is no available work around. (544551)
- When the VXLAN VNI mapping for a VRF is modified, paths towards one or more DPS peers may get updated incorrectly, resulting in loss of traffic towards

such peers.

Removing and re-adding the VNI mapping may fix this problem. (549493)

- Earlier when a static NAT profile is deleted from one interface it affected other interface where NAT is configured (560438)

DCS-7170 Series

- When a packet is mirrored to a GRE tunnel, the ECN value in the encapsulation IP header
of the mirrored packet may be intermittently corrupted. There is no workaround for this. (442457)

- NAT sync does not work reliably if the number of NAT connections are much higher
(in the order of 50K or more NAT connections). (506507)

- Monitor session with TX source to a port-channel may not be rate limited correctly. Link flap of the port channel may cause the mirrored traffic to stop. Workaround is to remove non-working port from port-channel. (516828)

- The issue is found if there is no space left to add new daisy chain entries but a change in the nexthop-group causes a need for a new entry. The BfnLoadBalancer agent can terminate if the server belonging to the entry that was supposed to be added to the daisy chain table goes down.

  If the issue is not resolved after agent restart it can be solved by toggling:
  load-balance server
  connection history source switch

  To:
  load-balance server
  connection history source server
  and back:
  load-balance server
  connection history source switch (527242)

- On config-replace or switch reboot with multiple VRFs configured and route cache enabled, some dynamic VLAN
related programming may be inconsistent and result in traffic being dropped. Workaround is to remove/reconfigure mapping or shut/no shut vxlan interface (537320)

- An adjacency change caused by a new server inserted in a nexthop group type VXLAN (nexthop group used by the stateless-load-balancer profile) failure due to resource exhaustion followed by a quick recovery (under 5

seconds) due to some other nexthop group releasing resources can lead to a BfnL3 agent restart. (543801)

- Under heavy l3 multicast route flaps, replication update may fail, leading to traffic drops. (620107)

DCS-7170 Series

- A MAP-T configuration that has a resolved exception offload nexthop, may transition to unresolved, even if the underlying route remains resolved in 2 cases:

  1) If the BfnSlice-FixedSystem agent restarts.
  2) If the MAP-T configuration is rapidly replaced with the same configuration, or a configuration using the same exception offload IP. (508539)

- The 7170 load balancer solution supports 512 L2 adjacencies. The usual topology usually uses 1 or 2 ecmp links to the next-hop router. If by mistake 512 L2 adjacencies are programmed and then the user tries to remove the incorrect configuration the adjacencies are not being removed. The workaround is to restart the BfnL3 agent. (515679)

- When a monitor destination is continually congested due to fan-in/high rates of traffic, and LAG is used in the system, the slice agent may restart when there is LAG membership change or port status change. (516260)

- A 7170 configured for MAP-T, may fail to reject map rules with duplicate IPv4 rule prefixes, resulting in continuous restarting of the BfnSliceAgent process until the offending rule is removed. The duplicate prefix check will fail to work if the map domain already has a configured "ea-length" and "psid offset". (537652)
  Series Affected: DCS-7170 Series

CCS-720XP Series

- If link speed is changed on a 2.5G interface, Strata forwarding plane agent may unexpectedly restart with "Process died with signal 3 \(SIGQUIT\)" signature. Subsequent restart of the Strata agent will be resolve the issue. (368424)

- The forwarding slice agent may restart unexpectedly when a SEU is encountered in the BSC_AG_AGE_TABLE during initialization. This may result in brief traffic outage. Switch is expected to start normal operation after the agent restart. (417588)

- When two or more hardware flow trackers are configured the forwarding agent may restart unexpectedly. In this case even if the extra flow tracker is removed the forwarding agent may continue to restart.

Workaround is as follows:
1) Do "shutdown" on the "flow tracking hardware"
2) Remove all flow trackers except one in the flow tracker config. Only one flow tracker can be present at a time.
3) Do "no shutdown" on the "flow tracking hardware"

In case the above doesn't work you need to remove flow tracking hardware by doing:
(config)# no flow tracking hardware
and reconfigure flow tracking hardware and add only one flow tracker. (426694)

- Authentication of any data device behind a tagged phone will fail after the phone is authenticated and authorised via EAP in phone VLAN on that port. Also, if a data device authenticates before tagged phone doing EAP, the authorisation of phone in phone VLAN will fail. (490365)

- On phone trunk ports which are not controlled by Dot1x, phones do not honour port-security max-address limit and get installed in the L2 table even after the port-security limit is breached (494095)

- NAS sends two EAPOL identity requests in response to EAPOL start from supplicants. This can cause authentication timeouts for some Windows supplicants. (498610)

- Executing ASU with phone trunk ports configuration can lead to Dot1x agent being killed. (503859)

- In case of WoL, with dot1x port in multi-host mode and dynamic vlan assignment,
  if an autheicated host is deleted with 'clear dot1x host mac ...', the host could
  no longer be waken up from the dynamic vlan. It could still be waken up from native vlan.
  Port shutdown/no shutdown would make waking up the host from dynamic vlan work again. (505855)

- Some front panel BASE-T interfaces might fail to forward traffic after a reload or linecard insertion (for modular systems), if they are configured with `speed 100full` command. The issue only affects the following 2.5GBASE-T interfaces:
  Et1,Et6,Et9,Et14,Et17,Et22,Et25,Et30,Et33,Et38,Et41,Et46,Et49,Et54,Et57,Et62,Et65,Et70,

  Workaround is to run `shutdown` followed by `no shutdown` on the affected interfaces. (519774)
  SKUs Affected: CCS-720XP-24ZY4, CCS-720XP-48ZC2 and CCS-720XP-96ZC2

- Front panel BASE-T ports might fail to link up due to PhyIsland agent restarting continuously.

Workaround is to reload or power cycle the switch. (523161)
SKUs Affected: CCS-720XP-24Y6 and CCS-720XP-48Y6

- Some BASE-T ports might report linkup; but fail to forward traffic after a reload or power-cycle.

  Workaround is to reload or power cycle the switch. (523649)
  SKUs Affected: CCS-720XP-24Y6 and CCS-720XP-48Y6

- If Dynamic authorisation request is sent with incorrect format of Calling-Station-Id then this may lead to ungraceful handling of the request. (548065)

- When hardware flow tracking is configured with "record format ipfix standard timestamps counters" (i.e. sw export), the IPFIX data packets generated by the hardware may get dropped on the CPU queue. The workaround is to increase the export interval by configuring "record export on interval <interval>". (552698)

- Link partners connected to the SFP28 ports with optics might see PCS/FEC errors, link flaps or failure to link up. (556805)
  SKUs Affected: CCS-720XP-24Y6 and CCS-720XP-48Y6

- While doing ASU, Dot1x Agent may restart unexpectedly if there were 802.1X supplicants present before ASU. (558476)

- Front panel BASE-T ports might stop forwarding traffic even though they are reported as linkup.

  Workaround is to run `shutdown` followed by `no shutdown` on the affected interfaces. (572686)
  SKUs Affected: CCS-720XP-24Y6 and CCS-720XP-48Y6

- Interfaces configured for MAC loopback are limited to 10 Mbps instead of the configured speed. (585395)
  SKUs Affected: CCS-720XP-24Y6 and CCS-720XP-48Y6

- 5GBASE-T ports might see symbol errors at 1Gbps if they flap after an SSU or after the forwarding agent restart.
  Workaround is to configure the affected ports with `speed forced 100mfull`, and then to revert this speed configuration. (593749)
  SKUs Affected: CCS-720XP-24ZY4, CCS-720XP-48ZC2 and CCS-720XP-96ZC2

- For a given tx-queue, traffic on unicast queue may starve the multicast queue. (616128)
  Series Affected: CCS-720XP Series

- Front panel BASE-T ports might fail to link up due to PhyIsland agent restarting continuously.

Workaround is to reload or power cycle the switch. (620854)
SKUs Affected: CCS-720XP-24Y6 and CCS-720XP-48Y6

DCS-7160, DCS-7170, DCS-7280R and DCS-7280R2 Series

- The AlgoMatch forwarding agent will restart when config replace is used to configure access-lists with large number of rules. (240540)
- Following a physical error on link between Jericho and Algomatch FPGA the SandHalo agent may restart, causing ACLs to be removed and reinstalled. (283917)
- When an acl configuration is applied to a large number of SVIs in a configuration session, the acl configuration fails. (367513)
- A SEU can occur on the Jericho side of the ELK interface to the AlgoMatch FPGA. These error interrupts can happen for other reasons like oversubscribing the ELK interface, but if they persist, they are usually the result of a SEU. This results in dropped control packets from SandHalo and SandHalo will unexpectedly restart continuously. A reboot or linecard reset is required to clear this condition. (486369)
  Series Affected: DCS-7280R2 and DCS-7500R2 Series
- Under certain conditions where small packet are bursting across many interfaces, chip can get in a state of dropping half packets coming into the chip. (488904)
- If the Scd agent unexpectedly restarts, FPGAs controlled by the agent could remain in an uninitialized state. The SandFap agent may then unexpectedly restart with a hardware initialization timeout error.

  A workaround is to configure "hardware access-list mechanism tcam". Doing so will have the side effect of disabling AlgoMatch. (501810)
  SKUs Affected: DCS-7280CR2A-30, DCS-7280CR2A-60, DCS-7280CR2K-30 and DCS-7280CR2K-60

7368, DCS-7300X, DCS-7500R and DCS-7800 Series

- When many IPv6 routes are configured and the BFD protocol in use, BFD sessions may flap when a linecard is removed or shut down. (279129)
- ManagementActive Agent repeatedly restarts and Management0 interface is not reachable in
  Modular systems. Doing switchover will address the issue. (369565)
- Hotswapping a card may cause a kernel panic and the switch will reboot unexpectedly. Not running traffic on the card before powering down will make this hit less frequently, but it may still hit. (387173)

- After linecard removal and re-insertion, lag member links may remain inactive due to "waiting for hardware to program port to RX (or receive)".

  Restarting the StrataLag agent recovers the port channels. (501496)
  Series Affected: DCS-7300X Series

- On modular systems with redundant supervisor cards, if the standby supervisor has connected management interfaces, ZeroTouch provisioning may fail to download a configuration from any connected DHCP servers. The workaround is to "shutdown" the management interfaces on the standby supervisor. (507185)

- During SSO, a fabric card's forwarding agent may experience an additional unexpected restart. In such cases, the forwarding agent will emit a "STRATA-3-RXDMASTUCKERROR" syslog message. A brief traffic outage may be observed. (572329)
  Series Affected: DCS-7300X Series

CCS-720XP Series

- PoE ports that are able to classify but do not power on for an extended period of time may cause Sysdb memory usage to grow, eventually resulting in out-of-memory events, particularly with TerminAttr

  A workaround is to configure "poe disabled" on the affected ports (528060)
  SKUs Affected: CCS-720XP-24Y6, CCS-720XP-24ZY4, CCS-720XP-48Y6, CCS-720XP-48ZC2 and CCS-720XP-96ZC2

DCS-7020, DCS-7280R, DCS-7280R2, DCS-7280R3, DCS-7500R, DCS-7500R2, DCS-7500R3 and DCS-7800R3 Series

- When the SandMcast and the SandFap agents are restarted, the VLAN floodset may not contain all the ports for several minutes. (67439)

- When in MLAG mode without ip routing enabled, under some control plane oversubscription scenarios the MLAG peer link might come down. The workaround is to either enable IP routing or have a static ARP entry on the MLAG peers for each other. (90247)

- An IPv6oGRE packet terminated using decap-group with a host route destination IPv6 address will be dropped.

  The workaround is to disable exact match host routes using "no platform sand ipv6 host-route exact-match". (95873)

- On DCS-7280E, DCS-7500E series, DCS-7050X, DCS-7250X, and DCS-7300 series switches, the vlan tag on IGMP messages(report, query, leave) generated by

the switch is not translated in the egress direction by the switchport vlan mapping command. (113104)

- Some packet loss may be observed when IP multicast traffic has high fanout on a single physical port (e.g. trunk port with many receivers for the same multicast group on different VLANs), even when the total egress packet rate is well below linerate. The default egress buffer settings may not perform well under this scenario. This issue can be resolved by adding "platform arad buffering egress port multicast max-queues-full 1" to the switch config and rebooting the switch. (115343)
- MAC mirroring ACLs do not match IPv6 packets. (137537)
- On a device with with a large number of active VLANs, doing "shutdown" and "no shutdown" on many interfaces may cause the SandMcast agent to restart. (175529)
- Mirrored traffic is not subject to egress security ACLs which are applied to mirroring destination ports. (190637)
- PBR is not supported along with IPv6 in IPv6 packets. (193914)
- On 100M interfaces acting as IEEE 1588 slave ports, restarting IEEE 1588 may cause ingress timestamps to spike by as much as 100s of ms.

  A workaround would be to reset the interface after restarting IEEE 1588. (218386)
- Acl and related features that use TCAM for rule matching do not work correctly on packets with IPv6 extension headers if the rules have layer 4 match criteria such as tcp flags and source/destination ports. (221161)
- If an ACL is attempted to be applied on a subinterface, whose parent port is not a routed port, the CLI will timeout. (229537)
- PBR policies applied on interfaces do not work if the interface has some subinterfaces that also have PBR policies applied. (243286)
  Series Affected: DCS-7020, DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series
- VTEP cannot learn a remote host's MAC address from VXLAN encapsulated IPv6 Neighbor Advertisement packets received from that host. This might be an issue in a pure IPv6 deployment where the VTEP does not receive any bridged traffic from the host. In such a scenario, the traffic toward the host will be flooded in the VLAN.

  The work around for this is to force Neighbor Solicitation (NS) packets from the host for its gateway or send bridging data traffic from the host. (246676)

- ACL/PBR/QOS will not take effect on ports with VLAN Translation configured. (246982)
- A TCAM profile not compatible with all linecards in a system will not be installed on any linecard in that system. However, hardware tcam profile status may show erroneously that the profile is installed on compatible linecards.

  Removing the incompatible linecard(s) or use a TCAM profile that is supported by all linecards in the system. (247842)
- VXLAN bridging traffic sent out of LAG interfaces may be temporarily dropped after an SSO event. (251398)
  Series Affected: DCS-7500R Series
- When linecards are powered on/off, there may be a traffic loss for a short duration on the interfaces where vlan mapping feature is configured. (254476)
- Unknown unicast and multicast packets are unnecessarily copied to CPU after VXLAN decapsulation when there is an SVI configured on the VXLAN VLAN. (258990)
- When a bidirectional PIM multicast receiver is connected to only one MLAG peer switch, the IGMP reports from the receiver may get dropped resulting in multicast traffic drops towards the receiver. (259308)
- Egress acl deny logging does not work when the packet is destined to a RFC5549 next-hop. (264045)
- When a DirectFlow flow is created with an action to drop the outer tag, the packet is still leaving the interface tagged. (264336)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- When a physical port (e.g. Et1) is removed from a Port-Channel (e.g. Po1) that has subinterfaces configured (e.g. Po1.1), and there are subinterfaces configured under that physical port (e.g. Et1.1), the subinterfaces under the physical port can be incorrectly programmed. This results in traffic being dropped for the incorrectly programmed subinterfaces.

  The workaround is the flap the subinterfaces affected. (269823)
- If one or more linecards in a modular system is running in tap aggregation mode, a small percentage of multicast traffic on linecards running in normal mode may be dropped, following a change to membership of some tap aggregation destination groups. (275286)
- After applying or removing shaping configuration on an L2 subinterface, the L2 subinterface must be flapped for the configuration to take effect. (278730)

- PIM multicast traffic may experience a brief interruption when one or more linecards on the same modular chassis enters or leaves TAP Aggregation mode. (279972)
- When the primary and fallback policy are both changed in the same config session, traffic may stop matching on either primary or fallback policy. (287146)
- When primary and fallback policies are both changed in the same config session, some packets will not be subject to either policy for a brief period during the configuration change. (287154)
- Power cycling a 7500E linecard in a chassis with 7500E fabric modules can cause packet loss on 7500R linecards. (295825)
- When both port-channel load balance for multicast and selective ingress replication is configured, groups that get ingress replicated incorrectly replicate packet to each member of port-channels that are member of the group.
  As a workaround one of the features has to be disabled. (344650)
- Ethernet over MPLS packets being terminated and decapped on a LDP pseudowire will be hashed as if the inner header is IPv4 rather than Ethernet (382763)
- If VXLAN is configured, PBR and QOS policies won't apply to traffic ingressing on a MLAG peer-link. (390804)
- Sometimes Macsec Proxy interface gets into error disabled state on reload when fips is enabled.

  To workaround the issue configure errdisable max flap value; i.e., "errdisable flap-setting cause link-flap max-flaps 24 time 10". Note the setting is global and affects non Macsec Proxy interfaces as well. (396589)
- When the DirectFlow 'priority' keyword is set greater than 65534 the configured priority will not be set to the correct value and the SandAcl agent may continually restart. (412206)
- With "ip pim spt-threshold infinity" configuration and having 10K or more Ipv4 (*,G) multicast routes, in addition to what hardware can accommodate, SandMcast agent may restart repeatedly. Work-around is to reduce the scale of (*,G) multicast routes to a number that can fit in hardware. (415164)
- Configuring 4094 different Egress IPv4 RACL on 4094 SVI will cause repeated SandAcl Agent crash.
  No workaround is available except for scaling down Egress IPv4 RACL. (415577)

- A switch reload with qos policy configured may result in SandAcl agent restart. (417935)
- Storm control maximum burst size is fixed to 10kB which can lead to storm control drops for bursty incoming traffic. (423231)
- With WRR scheduling on many ports and linerate across multiple traffic classes there can be a small amount of egress buffer drops. (425123)
- When the outgoing interface for a Vxlan underlay route changes from one forwarding chip to another, it can impact VXLAN overlay route convergence. (440233)
- Performing many updates to a PBR policy in a short amount of time may cause the SandAcl agent to restart unexpectedly. (441912)
- With VXLAN configuration, if the route to a remote VTEP churns while the tunnel hardware resource usage is closer to the hardware limits, then the SandL3Unicast agent might restart unexpectedly. (445834)
- V6 unknown multicast packets are not headend replicated to remote VTEPs. (448950)
- If an access-list is used in a PBR policy and also in a QOS policy, editing this access-list may result in a failure to apply the QOS policy. The workaround is to use two separate access-lists for the PBR and QOS policies. (450595)
- The SandFap agent unexpectedly restarts when a PRBS type unsupported by the interface is configured; this will lead to traffic loss on all the interfaces. (450978)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- VXLAN over a MACsec proxy port as underlay may stop forwarding traffic on reload. (451061)
- VXLAN routing over MACsec proxy port stops working when a proxy port that is not bound to an external interface is updated to be bound to an external interface. (455759)
- Sflow samples of VXLAN packets terminated by the switch, will not have their VXLAN headers stripped. (457096)
- "match nexthop-group" filter is not supported in PBR rules when the corresponding nexthop-group is referenced by ECMP routes. (458189)
- Internally duplicated CFM packet may cause double counting and duplicate replies towards the sender. (466833)
- On DCS-When a port-based connector is used for a pseudowire or local cross-connect patch, dot1q-tagged packets will have the outer tag incorrectly

removed on ingress/encap if any one of several other features are configured on the switch (on any interface) including: L2 subinterfaces, Dot1q Tunnel, Vlan Mapping, and Vxlan. The only workaround is to unconfigure these other features. (474093)
Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- SflowAccel does not send flow samples to collectors routed via BGP routes with additional backup paths. (476553)
- Once the maximum number of supported unique PBR policies per chip is exceeded, removing the PBR policy on an interface, converting the interface to a vlan member and applying a RACL on the SVI does not work. (477753)
- SandL3Unicast agent may leak memory when unshared nexthop group entries are modified repeatedly. (478158)
- When BGP Flowspec rules associated to a VRF are not programmed due to overflow in the number of supported VRFs, and the neighbor advertising those rules is brought down, the SandAcl agent may restart unexpectedly. (479587)
- Restarting the SandAcl agent while BGP Flowspec is applied on more than the supported number of VRFs can lead to unexpected traffic behavior. (481575)
- Local cross-connect patch panels do not function properly when any of the following features are configured on the system: L2 subinterfaces, Dot1q Tunnel, Vlan Mapping, Vxlan, and QinQ L3 subinterfaces. The only workaround is to unconfigure these other features. (485071)
- The SandAcl agent may crash if PBR is applied on SVIs during a linecard hotswap (486402)
- When BGP neighbors advertise Flowspec rules containing the police action and the system's policer resources are exhausted, any further change to Flowspec rules may cause the SandAcl agent to restart unexpectedly. Upon a SandAcl agent restart, existing Flowspec rules are removed from hardware and the system will attempt to program the new set of advertised rules, which will succeed if there are enough hardware resources.

  As a workaround, restart the SandAcl agent after freeing enough policer resources, e.g., remove rules from features such as QOS policies that use policer resources. (486688)
- TCAM bank reservation may not work after reload.
  The workaround is to remove and reapply the reservation config for any existing feature after all the SandFap agents are up. (488675)
- With a tcam profile configuration containing "feature tunnel vxlan routing", SandAcl agent restart may lead to another unexpected restart before the agent recovers. (492320)

Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- Once storm control is configured on an interface, policers configured via a QOS policy-map or cpu-traffic policy on this interface will police packets more aggressively than the configured rate.
  The workaround is to restart the SandFap agent.
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R, DCS-7500R2 (494749)

- If the SandFap agent is busy, or starved of CPU bandwidth, for an extended period of time, PTP stability may be affected negatively. The message 'TIMESYNC_ERROR' will be logged in syslog when this happens. (495418)

- Following an SSO event on an MLAG peer device with VXLAN configured, VXLAN split horizon rules might not be properly enforced. This can potentially create loops in the VXLAN network.

  One possible workaround is to restart the SandTunnel agent on the impacted MLAG peer device. (497551)

- Using a user defined TCAM profile that has the packet type `mpls ipv4 forwarding routed decap` may cause unpredictable behaviour in access control lists (ACLs) and IP TOS field corruption for ingress traffic that is not MPLS. (499458)

- "hardware next-hop fast-failover" is not supported with MPLS EVPN flood adjacency resolved over an MPLS SR tunnel that is in turn resolved over TI-LFA tunnel. (503263)

- In a 6PE configuration, packet ingressing on an L3 subinterface with explicit null label and destined to this switch is not supported. (504582)

- If the source IP is not in the routing table, the unicast RPF will not drop the packet and will forward a corrupted packet. (505285)

- Congestion discards keeps increasing for ports involved in fastdrop multcast routes where the incoming interface is a routed port or SVI with only one interface. (506369)

- On a modular system, if only some of the linecards are configured in Tap Aggregation mode, inserting or removing a linecard which is configured for Tap Aggregation would cause traffic disruption on other linecards in Tap Aggregation mode. (508024)
  Series Affected: DCS-7500R, DCS-7500R2 and DCS-7500R3 Series

- When a DirectFlow flow is modified, the original flow entry might still be programmed in the TCAM along with the modified one. The original TCAM entry will not be visible using CLI. The workaround is to manually restart the SandAcl agent. (508034)

- Removing a field-set configuration (i.e., via "no field-set ipv4 prefix <field-set-name>") does not cause traffic-policies that match on the field-set to be updated in the switch. Packets will still match on the IP prefixes or L4-ports of the removed field-set configuration. The removal of the field-set from hardware will take effect in a subsequent change to the policy configuration. (512073)

- Source MAC address is not learnt for packets that come in on interfaces with IPv6 uRPF configuration. (512737)

- With hardware accelerated SFlow enabled and more than 20 LAGs in the system and mirroring sessions configured, the Sand agent restarts continuously. (512973)

- Traffic for some routes may get mis-forwarded using default route under rare circumstances, that are influenced by some route distribution, and order of route updates. (513287)

- On a dut configured with subinterface with shape rate configuration, link flap may cause Sand agent to crash indefinitely until reload.

  System reload should resolve the issue (519535)

- Packets matching the deny rule in a Ipv6/Ipv4 Acl on L2 subinterface may not get denied due to inconsistency in the drop action for the Acls on L2 subinterfaces.
  There is no workaround for this. (521202)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7280R3, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R, DCS-7500R2, DCS-7500R3 and DCS-7800R3 Series

- TCAM entries may become corrupted when two CLI commands which read TCAM entries from hardware are executed simultaneously. The commands which cause a TCAM hardware read are 'show platform fap acl tcam diff', and 'show platform fap acl tcam hw hits`. (521356)

- On a scale setup, shape rate may not be able to apply on existing subinterfaces after SandFap resetart and no shape rate may not be able to configure on new subinterfaces.

  Dut reload is needed to allow shape rate to apply on the subinterfaces. (521812)

- SandFap agent restart or a "config replace" operation may cause some subinterfaces to transition to "notconnect" state.

  "shut/no shut" the parent interface or the affected subinterface to bring the subinterface back up. (535787)

- Ipv6 multicast routes with IIF as port-channel subinterface may remain unprogrammed after reloading the peer switch to which the IIF is connected.

  Workaround is to clear the affected routes or flap the affected IIF. (537653)

- With hardware fast failover configuration, ECMP to non-ECMP FEC transition leads to programming of backup path in hardware even when the active path is up. (540338)

- Routed traffic may be continuously dropped after all SandFap agents restart. The workaround is to restart SandL3Unicast agent. (540586)

- An over-voltage condition on the POS1V2_HBM_IO_JE0 power rail can cause the system to power-cycle. (544659)
  SKUs Affected: DCS-7280CR3-96 and DCS-7280CR3K-96

- In configurations involving IP/IPv6/MPLS routes resolved multiple IS-IS-SR tunnels (including indirectly via other tunnels such as BGP-LU) an IS-IS-SR tunnel failure on a remote node (such as Loopback shut, or device reset) may cause extended loss on other nodes as reconvergence occurs as the multi-path set is updated. The loss duration will vary depending on the number of resolution BGP-LU tunnels and on the number of internal VLANs (run "show ip int brief | wc -l" to get an estimate of this number) and could be on the order of 30 milliseconds per tunnel, if the VLAN count is on the order of 2000, and if both IPv4 and IPv6 routes are in use.

  A workaround may be to try to reduce the number of BGP-LU tunnels, or to manually adjust the network configuration to divert traffic from the IS-IS-SR tunnel towards the device to be reset. (546432)

- Egress sFlow will not sample BPDU packets originating from the local CPU (548170)

- 'Persistent Internal Drop DeqDeletePktCnt' error messages are seen due to incorrect/missing system ACEs. Hitful restart of SandAcl agent is needed to resolve the issue. The trigger for this issue is unknown. (548524)

- LAGs with VLAN translation configuration may experience brief misforwarding of packets to incorrect VLANs during LAG member flaps.

  A workaround is to avoid overlapping customer and bridging VLANs in the VLAN translation configuration. (553890)

- For interfaces with both a primary and fallback PBR policy applied, a policy update containing multiple ACL updates could cause packets to miss both the primary and fallback policy during the update. (562198)

- If a QoS policy with rules of different ACL types fails to program in hardware for one of the ACL types, the subset of rules that was programmed

successfully may not match incoming traffic correctly if other QoS policies are configured and applied in the system. (571599)

- BGP Flowspec policies may stop working correctly if the feature is applied on multiple VRFs and either the configuration is removed and -reconfigured repeatedly, or the BGP neighbor removes all advertised rules and then re-advertises them. (571601)
- Link local packets in an MLAG Campus AP setup can result in duplicate packets, or a forwarding loop if there are multiple MLAGs in the topology.

  Workaround: The loop can be mitigated by running `shutdown` on interface Vxlan1 on each peer in each MLAG. (573509)
- A config-session that applies primary policy to an interface and updates ACLs/classes used by the primary policy may lead to the policy to not be programmed correctly in hardware if the interface(s) where this policy is applied is/are also covered by a fallback PBR policy. (578146)
- When 'ip-length' key field is missing from the "ipsec" TCAM feature in the operational TCAM profile, all traffic on the IPsec tunnels may be trapped to the CPU, leading to low tunnel throughput.

  The workaround is to enable the 'ip-length' key field in the "ipsec" TCAM feature. (588127)
  SKUs Affected: DCS-7020SRG-24C2, DCS-7020SRG-24C2-F and DCS-7020SRG-24C2-R
- On a shaped subinterface tx-queue, configuring the bandwidth doesn't take effect unless no-priority is also configured. (588133)
- Adding a new member into a LAG with a high-scale VLAN translation configuration may cause some packets to be misforwarded to incorrect VLANs.

  A workaround is to keep the new LAG member administratively shut before configuring it into a LAG. After a few seconds, unshut the member. (588883)
- In BGP Flowspec configurations with large number of matches and significant amounts of churn in the requested matches, incorrect actions may be applied to the matched packets. (592765)
- When a shape rate is configured on a subinterface, restarting the Sand agent may cause the Sand agent to unexpectedly restart continuously.

  A workaround is to reload the system. (593144)
- When a PBR policy is applied to an SVI and new chips are added to the system, PBR may not work for the interfaces associated with the new chip if a policy is ever applied. (607599)

- In an EVPN MPLS configuration, changing the membership of an interface from port-channel A to port-channel B might result in incorrect forwarding to/from pre-existing members of channel group B.

  The workaround is to unconfigure the pre-existing members from being part of the port-channel and then configure them again. (610316)

- While in Tap Aggregation mode, traffic forwarding may be disrupted on two-way (tap-tool) ports following a stateful switchover or a Mirroring agent restart. (614967)

- A tcam profile change in flex-route, cbf, or egressIpv6Racl features may lead to forwarding issue. Restarting the SandL3Unicast agent would recover from the problem. (617588)

- With the configuration "ip hardware fib next-hop rfc5549 dedicated", IPv6 egress ACL may be skipped if IPv6 route is changed from drop to forwarding. (619336)

- If 'cpu traffic-policy <policyName> vrf all' is configured, where the traffic-policy contains rules with the policer action, and the operating TCAM profile does not support the CPU traffic-policy feature, then configuring any routed port in the switch may lead to an unexpected SandAcl agent restart. The workaround is to remove the 'cpu traffic-policy <policyName> vrf all' configuration. (619998)

- Postcard sampling doesn't work for traffic that is forwarded out of a sub-interface that has shaping applied. (621932)

DCS-7280R and DCS-7500R Series

- In MPLS L2EVPN configuration, traffic requiring 3 or more LU labels to be pushed, may not be forwarded correctly. (275834)

- On the 7500R-8CFPX-LC linecard modules, rapid removal and reinsertion of the transceiver may result in the Denali agent restarting.

  Inserting transceiver 10 seconds after removal from the same slot is the workaround. (293594)
    SKUs Affected: 7500R-8CFPX-LC

- VRF-mapped IP over MPLS packets with TTL=1 in the IP headers may be dropped, if the installed system TCAM profile uses packet types 'mpls ipv4 forwarding routed decap' or 'mpls ipv6 forwarding routed decap'. This could be a predefined TCAM profile such as pbr-match-nexthop-group or a user-defined profile with these packet types.

  Create a new TCAM profile based on current profile and remove these packet types from all applicable features. Note that this will remove support for

these packet types in egress ACLs, and 'mpls tunnel termination model ttl uniform dscp pipe' configuration will no longer work. (412811)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- Configuring more than 6 MPLS labels for the pseudowire path (including VC label and flow label), will cause the SandTunnel Agent to crash and not recover. The only workaround is to reduce the number of transport labels and/or to remove flow label such that the total is 6 or fewer. (443140)

- When an ingress Port Acl includes TCP or UDP port range matches and vxlan is configured on the switch, any vxlan transit packet ingressing into the switch may incorrectly match on such rules. To prevent this, key field l4ops must be excluded from the tcam profile. (477195)

- Optimized routes may not be programmed properly if TCAM profile is changed from <profile-1> to <profile-2> with both profiles having 'feature flex-route' in it.

  The workaround is to change the TCAM profile in two steps - first change from TCAM profile <profile-1> to default and then from default to <profile-2>. (483629)

- With VXLAN, and PIM configuration on overlay SVI, VXLAN packets with inner IPv6 multicast packet consisting of Hop-by-Hop option may not be terminated and forwarded correctly. (484825)

- When MACsec is enabled and a SSO failover occurs, the Evora agent may restart due to "LMI Access timeout", which may cause links to flap resulting in extended traffic loss. (494072)
  SKUs Affected: 7500RM-36CQ-LC

- In an EVPN MPLS configuration, extra invalid packets may be sent out during flooding of a BUM packet in an EVPN MPLS VLAN which may cause loops in the topology.

  The workaround is to restart SandL3Unicast agent. (498762)

- EVPN MPLS with implicit null tunnel underlay is supported only when MPLS tunnel counters are enabled. (500298)

- When an SVI is configured with an MTU value and a new interface is created with breakout cable and configured to be in that vlan, the new interface is not programmed with the correct MTU value. The workaround is to re-apply the MTU configuration on the SVI. (536927)

- IPv4 ECMP does not work if TCP MSS clamping is enabled on any or all of the egress interfaces have TCP MSS clamping enabled in hardware MSS clamping mode. All traffic would flow through one of the ECMP paths.

Workaround : Restart SandL3Unicast agent if TCP MSS configuration is modified on any of the interfaces in the switch. (538642)

- IQM_RST_USCNT_ERR, IQM_FR_FIMC_DB_ROLL_OVER, IQM_FR_MNMC_DB_ROLL_OVER interrupts of Jericho chip indicate traffic to and from ports of the affected chip to be dropped. A full reset of the chip could workaround this issue. (540881)
- Reloading a switch in Tap Aggregation mode with multiple large tool groups (35 members or more) and continuous ingress traffic may result in the forwarding chip's multicast buffer being locked up; this will causing some traffic to not be forwarded.

  A workaround is to reset the affected forwarding chip with the CLI command "reset platform fap full". (547590)
- If the forwarding agent is restarted after configuring a service profile on an interface, the forwarding agent may continuously restart unexpectedly.

  A workaround is is to remove the service-profile and re-add it. (549335)
- When a device with VLAN translation entries configured on LAGs where the VLAN tag matching rules overlap with bridging VLANs on the same LAG is rebooted, there may be a window of time in which packets are mapped to incorrect bridging VLANs (571307)
- An interface with a link down debounce of less than 1.5 seconds configured may not respond to a local fault deassertion at the physical layer fast enough causing the link to spuriously flap.

  Workaround is to configure a longer link down debounce time. (571797)

DCS-7280R2 and DCS-7500R2 Series

- If there is a parity error in the PPDB_B block of a JerichoPlus or QumranAx chip, the router MACs pointing to the CPU may get deleted from the hardware MAC table on that chip leading to loss of L3 connectivity.

  As a workaround, restart the SandMact agent using the CLI "agent SandMact terminate". (521075)
- Under high ambient temperature conditions, the switch may reboot due to a critical system temperature. (544313)
  SKUs Affected: DCS-7280CR2A-60-F and DCS-7280CR2K-60-F
- Multicast traffic on non-default VRF will be lost for as long as 15 minutes when default VRF is multicast enabled without any L3 interfaces.
  Workaround is to disable mulitcast on default VRF or configure a dummy L3 interface. (619693)

DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series

- During restart of SandAcl agent, packets may not be subjected to ACL rules for a short period of time. (372971)
- Neighboring interfaces may flap if speeds or speed groups are configured on an interface. (394764)
- The supervisor may fail to negotiate the network link connecting active and standby. Symptoms include a standby failing to complete reboot after reload. (459690)
  SKUs Affected: DCS-7800-SUP
- The SandFapNi agent may restart continuously preventing ports coming up. (462680)
  SKUs Affected: DCS-7280CR3-96, DCS-7280CR3K-96, DCS-7280DR3-24, DCS-7280DR3K-24, DCS-7280PR3-24 and DCS-7280PR3K-24
- The SandDanz Agent may restart a number of times when applying a configuration with a large number of tap or tool ports, or when adding, removing or modifying a tap or tool port configuration while a large number of destinations are configured. (472094)
- Speed change on a port with running traffic may lead to stuck queues for packets egressing on that port. If this occurs, shut the port and restart SandFapNi agent to recover. To avoid this, shut the port before changing speeds. (479144)
- PBR, QOS, and CPU policies applied to a VLAN interface will not function correctly on untagged packets ingressing trunk ports mapping to a native VLAN equaling that of the VLAN interface. (483364)
- Outer DSCP is not derived from Traffic Class in VXLAN encapsulated bridged packet. (487274)
- PBR, QOS, CPU policies applied to VLAN interfaces may not function correctly if VLAN interface memberships change during SandFapNi restart, Linecard insertions or removals, or during interface speed changes.

  The workaround is to restart the SandTunnel agent, or reapply the policy configurations. (488958)
- If tap aggregation and a CPU traffic policy are configured together, either the CPU traffic policy will not apply to any traffic or the SandAcl agent will continuously restart. (492549)
- With large Nexthop group updates, in rare instances Packet can egress with wrong header data. (499845)

- On QSFP ports with the CRT50216 PHY, configuring 50G-2 on the /1 and /3 may result in the /1 flapping 1 or more time. (500018)
- Configuring 513 different Egress IPv6 SubInterface ACLs will cause repeated SandAcl Agent restarts. No workaround is available except for scaling down Egress IPv6 SubInterface ACLs. (502185)
- If same IP/IPv6/MAC ACL is applied on a front panel port or Port-channel and a subinterface of that port or port-channel, then the behaviour will depend on the order in which the ACL is applied on these interfaces. The ACL may not actually be applied if ACL is applied first on at least one of the subinterface and then on the parent interface. Also, it is not possible to remove ACL configuration from the parent interface using 'no <ip/ipv6/mac> access-list <aclname> <direction>'. Configuration can be removed using 'configure replace'. Workaround is to use different ACLs (may contain same rules) on parent and its subinterfaces. (503650)
- Replacing a linecard with a different type of linecard while the switch is live will cause the SandFapNi agent to crash. Rebooting the switch will recover the problem. (503896)
- When a Gratuitous ARP (GARP) that maps an IP address to a special multicast MAC is received with another packet, the system can restart unexpectedly due to a kernel crash. (504140)
  Series Affected: DCS-7280R3 and DCS-7800R3 Series
- After several re-insertion of a line or fabric card, fabric serdes of the card can all become disabled causing all packet drops to or from a linecard with no connectivity. (504370)
  SKUs Affected: 7500R3-24D-LC, 7500R3-24P-LC, 7500R3-36CQ-LC, 7500R3K-36CQ-LC, 7800R3-36D-LC, 7800R3-36P-LC, 7800R3-48CQ-LC, 7800R3-48CQM-LC and 7800R3K-48CQ-LC
- In interface traffic-policies, when configuring a destination port after configuring source port field-set, the ports are treated as field-set names (506962)
- VXLAN transit packets received on the MLAG peer-link can be misforwarded or dropped. (512214)
- If an IP/IPV6 or MAC ACL is removed from an interface, physical or logical, with the exception of vlan interfaces, after a SandAcl restart, then traffic on that interface may continue to hit the ACL if the ACL is still configured on any other interface or it may hit some other ACL even though that ACL is not configured on this interface. (516000)
- Packets that exceed the configured L3 MTU are still subject to TX mirroring. (516199)

- Using copper cables at interface speeds 400g-8, 200g-4, 100g-2 or 50g-1 may experience occasional FCS errors. (516663)
  SKUs Affected: 7500R3-24D-LC

- If a MLAG LAG member is unconfigured while the SandAcl agent is not running, BUM traffic from the peerlink to the specific member may be dropped.

  The work around is to reconfigure and unconfigure the MLAG LAG member while the SandAcl agent is running. (516712)

- If a LAG with some subinterfaces configured with ACLs is deleted while SandAcl agent is shutdown, the ACL applied on such subinterfaces will continue to apply even after removing the ACL configuration on such subinterfaces. (519537)

- Parity Interrupts for the first bank of first Fap of TCAM sometimes cause corruption in MLAG entries in the Large Exact Match table. This can be detected using the TCAM interrupt counter increase. Restarting of DUT recovers from the problem. Alternatively, one can change the TCAM profile and change it back. There is no work around to this , except to recover back. (519945)

- With IS-IS SR resolution over TI-LFA configuration, SandL3Unicast agent might restart unexpectedly during TI-LFA tunnel churn. (521187)

- When two or more of the following features: Port ACL, PBR, QoS, Flowspec, Aegis, and CPU Policy are applied on the same interface with a non-default TCAM profile, one or more of the features may not work (526913)

- If the "acl subintf ip/ipv6/mac" feature is added to a TCAM profile without the corresponding "acl port ip/ipv6/mac" feature being added to the same profile, subinterface ACLs will not work. (532393)

- When PBR/BGP Flowspec/QoS/CPU policies are applied on SVIs, and the linecard of one of the SVI members gets removed and re-inserted, the SandAcl agent may restart unexpectedly.

  A workaround is to remove the SVI member before its linecard gets removed and re-inserted. (532575)

- MTU violating VXLAN routed packets with either IPv6 overlay or an Ethernet tag on the underlay ethernet header can cause the egress port to lock up. When in this state, no packets will egress the port and traffic will get deleted on the ingress VOQ. Shutting and unshutting the port will restore the traffic. (537323)

- Disabling of egress RACL sharing ("no hardware access-list resource sharing vlan ipv4 out") is not supported with MPLS swap routes that are optimized as

forward routes. The workaround is to re-enable egress RACL sharing, which is the default option. (542197)

- SandL3Unicast restart causes traffic disruption for packets forwarded through Tap Aggregation or L2Subinterface. Restarting SandTunnel would recover from the condition. (545513)
- The "phy diag test pattern" CLI being in the startup-config after reboot can cause the forwarding agent to restart repeatedly. (547015)
- A VXLAN packet that would be bridged, after decapsulation, to the same interface as it ingressed will be dropped instead of being bridged. (549785)
- MPLS tunnel terminated GRE-over-IPv6-over-MPLS packets are forwarded incorrectly. (550842)
- When using the "traffic-policy-cpu-port-flowspec-qos" TCAM profile, system ACLs and traffic-policies that match on fragmented packets will not work correctly. (556077)
- When MLAG Fast MAC Redirect feature is enabled, transient traffic loop may happen when MLAG interfaces go to partially active state (558533)
- When VXLAN is enabled, L4 port match in ACLs on VXLAN decap packets does not work. (567246)
- Upon recovery from a PFC pause storm, Normal transmission of PFC frames on the interface and traffic class where we received the pause storm will not resume.

  Workaround: To restore PFC functionality, disable and re-enable PFC on that interface. (571168)
- PTP packets may be incorrectly processed if they are forwarded by a switch when PTP is not enabled on the switch, or if the switch is running a version of EOS that does not support PTP on the particular hardware platform.

  A workaround is to configure the packet forwarding engine to pass through PTP packets without modification using the following commmand: "platform fap diag mod IPPB_IEEE_1588_IDENTIFICATION_CAM 0 32 VALID=0" (573072)
- ECN may not work correctly for packets destined for tx-queues that were detected as stuck by PFC watchdog, even after watchdog recovery. The workaround is to remove and reapply the ECN config for the affected tx-queue. (573366)
- On a device with VXLAN configured, a large number of split horizon drops may result in some packets being discarded on neighboring devices due to CRC errors (574067)

- "hardware next-hop fast-failover" is not supported along with VXLAN configurations. (574632)
- When an interface traffic-policy is changed such that hardware resources are exhausted by the change, SandAegis agent may restart. After the agent restart, the switch will recover after traffic-policy rollback kicks in. (574639)
- Configuring an IPsec encryption algorithm with a key length less than 256 bits can result in a B52 agent crash. (610799)

DCS-7020 Series

- When multiple Ipsec tunnel interfaces are shutdown, then "no shut" in a short period of time, routes associated with some tunnel interfaces may not be installed after "no shut". The workaround is to do shut/no-shut again on the individual tunnels where routes not installed. (377984)
  SKUs Affected: DCS-7020SRG-24C2-F and DCS-7020SRG-24C2-R
- When traffic is flowing from a 10G interface to a 1G interface and PFC is enabled on the ingress 10G interface, if the administrator changes the COS to TC mapping all the incoming traffic on the 10G interface is dropped. The only way to recover is by restarting SandFap. (400653)
- The SandIpsec agent does not automatically restart after a TCAM profile change, which means that IPsec-related changes to the profile will not take effect.

  The agent must be manually restarted after the TCAM profile is changed using "agent SandIpsec terminate". (567183)
  SKUs Affected: DCS-7020SRG-24C2, DCS-7020SRG-24C2-F and DCS-7020SRG-24C2-R
- When IP packets small enough to require ethernet padding are forwarded into an IPsec tunnel, the padding bytes are not stripped. This may cause these packets to be dropped when decapsulated and decrypted by other IPsec products. (603398)
  SKUs Affected: DCS-7020SRG-24C2, DCS-7020SRG-24C2-F and DCS-7020SRG-24C2-R

DCS-7500R3 and DCS-7800R3 Series

- If the SandFabric agent restarts, it may continually restart.

  The workaround is to power cycle the fabric card. (435103)
- In some situations, some fabric links going to a fabric chip are not used to carry fabric traffic. (450214)

- Traffic on a subinterface will be subject to BGP Flowspec matches applied to the parent interface, unless the TCAM profile has the flowspec feature configured with 'port qualifier size N', where N > 1. (541950)
- Configuring multiple DirectFlow flows of different priorities at once may restart the SandAcl agent continuously. A workaround would be to configure the DirectFlow flows one after the other. (543622)
- The flexroute feature may override the forwarding decisions from PBR policies and BGP Flowspec matches. (544872)
- When a line card is swapped with a different model line card, and there was previously some LAG configuration for ports that do not exist on the new line card, the SandFap slice agent corresponding to that line card may restart repeatedly.

  A workaround is to re-insert the old line card and wait approximately two minutes. Then, re-insert the new line card. (545221)
  Series Affected: DCS-7500R and DCS-7500R2 Series
- Routed packets may not be forwarded correctly when L2 subinterfaces are configured. (559712)
- MPLS Pseudowires with Flow-Aware Transport Label (flow label) enabled may incorrectly encapsulate with a flow label value in the reserved 0-15 label range. (560378)
- The Arp agent may continually restart when hardware accelerated sFlow is enabled.

  Toggling sFlow, i.e. "[no] sflow run", may fix the issue. (571099)
- PVLAN over VXLAN is not supported on MLAG devices. (587536)
- SandAcl agent may restart when programming flows at many different priorities. Workaround is to limit the number of different priorities to 1024. (588420)
- In an EVPN MPLS multihomed configuration, packets egressing towards non designated forwarder ports may not be dropped. (592102)
- With a port without any explicit speed configuration, many removals and insertions of a 1G transceiver in an SFP+ or SFP25 port, or of a 40G transceiver in a QSFP100 port, may cause the forwarding agent to restart and all links to flap.

The workaround is to apply a speed configuation on the port matching the supported speed of the inserted transceiver. (600618)

- With MLAG fast MAC redirection enabled, if one of the LAGs in the MLAG is down then a packet whose DA is either the broadcast MAC or the MAC is unknown, the packet may be double delivered or loop continuously.

  The workaround is to disable the MLAG fast MAC redirection feature in "config-mlag" mode:
  inactive mac-address destination peer-link direct (605211)

- Continuous SflowAccel agent restart is seen when hardware sFlow and shaping on LAG subinterfaces is configured. This will result in hardware sFlow not working as expected. (610518)

DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series

- With sustained high MAC scale, hardware learning of L2 MACs may get disabled leading to flooding.

  When this condition occurs, a workaround is to clear the MAC table (clear mac address-table dynamic). (488731)

- When using 64-bit versions of EOS, enabling auto-negotiation on any non-BASE-T interface will cause the forwarding agent to restart.

  The workaround is to configure forced speed. (522773)

- When a line card is swapped with a different model line card, and there was previously some LAG configuration for ports that do not exist on the new line card, the SandFapNi slice agent corresponding to that line card may restart repeatedly.

  A workaround is to re-insert the old line card and wait approximately two minutes. Then, re-insert the new line card. (536443)
  Series Affected: DCS-7500R3 and DCS-7800R3 Series

- On large systems with more than 4 linecards, the SandCounters agent may restart continuously. (536744)
  Series Affected: DCS-7500R3 and DCS-7800R3 Series

- Under sustained heavy load, when more than one interface is receiving traffic at linerate capacity, the SandCounters process may restart repeatedly until traffic is reduced. (543931)

- In the presence of virtual MAC with mask configuration, packets that undergo recirculation may not be properly forwarded. (559242)

- When an interface traffic-policy containing both IPv4 and IPv6 match rules is applied to one or more L3 interfaces with a valid IPv4 and IPv6 addresses later has all IPv4 or IPv6 match rules removed results in the traffic-policy no longer being applied to the interfaces.

  Workaround is to re-install the policy on all interfaces (574937)

- In scaled traffic-policy scenarios, when using more than half the tcam capacity on the same FAP,
  adding, deleting or modifying a traffic-policy can time-out and cause a CPU spike for an extended
  period of time (like 3-4 minutes).

  The workaround for this problem in case it does not recover on its own is to restart SandAegis agent. (577206)

- After a config replace LAG members may start dropping all untagged ingress packets due to dropVoqInPortNotVlanMember.

  To work around, remove the interface from the LAG and then add the interface back in the LAG. (578380)

- When inserted into a previously-occupied linecard slot, Linecards may boot-up with many interfaces not connected and the "error-correction encoding" CLI command not having any effect.

  Workaround is to power cycle the linecard with the "no power enable" and "power enable" CLI commands. (599945)
    SKUs Affected: 7800R3-48CQM-LC

DCS-7280R and DCS-7280R2 Series

- VXLAN packets that are decapped and bridged are incorrectly subject to the IP ACL applied on the ingress port. (221457)

- When ACLs are applied on a large number of interfaces (more than 1000 SVI interfaces), the SandHalo agent may restart with a SOCKET_CLOSE_LOCAL syslog message. (253015)

- IPv6 routing with virtual VTEP configuration will not work on platforms that run in AlgoMatch mode. Workaround is to change the access-list mechanism configuration to tcam (472142)

- RACLs are not supported for VXLAN traffic ingressing on a MLAG peer-link when AlgoMatch is enabled. (485677)

- For an ACL applied to a LAG subinterface when all members of the LAG subinterface on a given chip are down, subsequent edits to any ACL on that chip may cause the default configured action to be applied to all interfaces

on the chip where an ACL is present.

The default configured action is to either drop or permit if the "hardware access-list update default-result permit" is present.

To recover when this bug:
- Remove the "ip access-group" configuration from LAG subinterfaces that are down
- Remove the LAG members that are down from the LAG that has subinterfaces with an ACL configuration (598255)

7300X3, 7320X, 7368, CCS-720XP, DCS-7010, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7060X4, DCS-7250X, DCS-7260X, DCS-7260X3 and DCS-7300X Series

- In multi-chip systems with L2 MTU greater than 9236, packets that are larger than 9236 bytes that flow between the switch ASICs will be dropped. (102837)
  Series Affected: 7300X3, DCS-7250X, DCS-7260CX and DCS-7300X Series

- Traffic streams matching DirectFlow flows with VLAN or MAC rewrite actions could face brief disruption across a StrataL3 agent restart. (111833)
  Series Affected: DCS-7050X Series

- When performing reload hitless, link flaps on BASE-T ports might be observed. (152459)
  Series Affected: DCS-7050TX Series

- MAC ACLs and PACLs cannot co-exist on the same interface if QoS policy ACLs exist in the switch (186949)

- The StrataVlanTopo agent may unexpectedly restart after many linecard online insertion and removal operations. (193787)
  Series Affected: DCS-7300X Series

- Ethernet65, Ethernet66 may experience extra link flap when performing fast boot. (221059)
  SKUs Affected: DCS-7260QX-64-F, DCS-7260QX-64-R, DCS-7260QX-64-SSD-F and DCS-7260QX-64-SSD-R

- The Strata fabric or linecard agent may restart due to fabric link flaps leading to traffic outage. (225302)
  Series Affected: 7320X and DCS-7300X Series

- DirectFlow flow in table type vfp will not match malformed Arp requests. (233922)

- When traffic is redirected using PBR and when the FIB lookup based on destination IP address indicates ARP miss, the PBR redirected traffic may be

rate-policed.

The workaround is to use count action for the ARP-needed class. (238084)

- When the utilization of the MAC address table grows close to the full hardware capacity, the StrataL2 agent may encounter an out of memory (OOM) condition in the system, causing the agent to get restarted. (238115)
  Series Affected: 7320X, DCS-7010, DCS-7050TX, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7260X, DCS-7260X3 and DCS-7300X Series

- If nexthop resources are exhausted as indicated by syslog VXLAN_HWHER_NEXTHOP_RESOURCE_FULL, forwarding of BUM traffic to that VTEP will be affected. (246391)
  Series Affected: DCS-7050X and DCS-7060X Series

- During an SSO failover, Strata Fabric agent may not detect hardware, resulting in a fatal error reboot with increased traffic outage. (250129)
  Series Affected: DCS-7300X Series

- In an L3 EVPN setup, traffic that is sourced by a VTEP that is a pure VXLAN router (i.e., it performs no VXLAN bridging and has no hosts attached to it) might incur some loss at the receiving VTEP, where the packets are decapsulated and forwarded.

  Configure a custom PDP policy with the vxlan-vtep-learn class set to count to work around this issue. (251117)

- BUM traffic may temporarily loop into the MLAG pair when a member interface in either the peer-link port channel or in an MLAG port channel is brought up. (259213)

- When IPv4 uRPF exceptions are already programmed, configuring IPv6 uRPF exceptions imposes a heavy processing load on the Strata Slice agent to do a transition from IPv4 to IPv4-v6 exception mode in the hardware. Therefore, under a scaled config scenario, the Strata Slice agent may restart repeatedly.

  Removal of IPv6 exceptions will help in recovering the system if this condition is hit. (264449)

- IS-IS configured over LAGs may see neighbor adjacency flapping during a hitless restart. (276232)

- A PCI error can break counter collection for an ASIC.

  Resetting the ASIC with "platform trident reset" will fix this error. (277519)

- After hitless speed change from 1G to 40G or 100G, link may remain down.

  Workaround is to perform hitful restart of forwarding agent. (283175)
  SKUs Affected: DCS-7050CX3-32S, DCS-7050CX3-32S-F, DCS-7050CX3-32S-R, DCS-7050SX3-48YC12, DCS-7050SX3-48YC12-F, DCS-7260CX3-64, DCS-7260CX3-64-F and DCS-7260CX3-64-R

- Applying a large configuration containing many interface changes may result in Strata forwarding agent restart, which could cause traffic loss during the reconfiguration. (330840)

- Some ports (esp. Et73-Et96 and Et103-Et104) might blackhole traffic or fail to linkup. (358361)
  SKUs Affected: DCS-7050TX-128-F, DCS-7050TX-128-R, DCS-7050TX-128-SSD-F and DCS-7050TX-128-SSD-R

- When VXLAN is configured and when a route or ARP points to an ecmp group with both local and remote nexthops, then a packet destined to this ecmp group may get looped between the linecards and fabric cards resulting in link congestion and packet drops. The work around is to disable the source port based hashing by removing "ingress-interface" in "ip load-sharing trident fields" command. (368073)

- Irrespective of IGMP snooping being enabled or disabled, IGMP packets will not be flooded to remote VTEPs. (368106)
  Series Affected: 7300X3, DCS-7050X2 and DCS-7050X3 Series

- DirectFlow entries that redirect traffic out of a port-channel may incorrectly egress packets on none or multiple members of the port-channel. (378467)
  SKUs Affected: DCS-7250QX-64-F, DCS-7250QX-64-R, DCS-7250QX-64-SSD-F, DCS-7250QX-64-SSD-R, DCS-7260CX-64-F, DCS-7260CX-64-R, DCS-7260CX-64-SSD-F, DCS-7260CX-64-SSD-R, DCS-7304, DCS-7308 and DCS-7316

- After switching scheduler mode, the StrataCounters agent might be unable to complete a hitless reload shutdown stage, which will cause a hitless reload to be hitful. This can be pre-identified by seeing "SBus ack error in schan command" in the StrataCounters agent log. Workaround is to reset the ASIC before running reload hitless. (388694)
  Series Affected: DCS-7050X3, DCS-7060X, DCS-7060X2 and DCS-7260X3 Series

- DHCP unicast packets which are not destined to switch are copied to CPU, which may forward the packet to destination along with one copy forwarded in hardware. This results in duplication of unicast DHCP packets. (393520)

- Having any ACLs with UDF qualifiers as well as any of the following LAG/ECMP hashing features present in the configuration: RRoce hashing, flexible hashing or TTL/HopLimit hashing, will result in incorrect operation of the LAG/ECMP hashing where the switch incorrectly hashes on IP payload. To

avoid this problem the conflicting features should not be configured at the same time. (403182)
Series Affected: DCS-7050X, DCS-7050X2, DCS-7060X, DCS-7060X2, DCS-7260X3 and DCS-7300X Series

- Changing PFC Watchdog configuration while traffic is flowing can result in sub-second traffic outage when PFC Watchdog is in non-disruptive mode and multi-second traffic outage when PFC Watchdog is in disruptive mode. (403790)

- Switch may drop ingress UDP traffic destined to the switch MAC address when destination UDP port of the ingress packet matches VXLAN protocol default UDP port even if the destination IP address of the packet does not match any of the configured local VTEP IP addresses. (404138)
  Series Affected: 7300X3, CCS-720XP, DCS-7050X2 and DCS-7050X3 Series

- DirectFlow flows with mirroring action may not be reprogrammed after a supervisor switchover or StrataMirror agent restart.

  The workaround is to restart the Strata agent, which restores the flows. (406857)

- Irregularities in processing 802.1q packets (407644)

- Restart of StrataL2 may lead to continuous StrataL2 restarts. Workaround is to reload the system. (408138)

- DirectFlow flows do not take precedence over conflicting router ACLs. (408734)
  Series Affected: 7300X3, CCS-720XP, DCS-7050CX3, DCS-7050SX2, DCS-7050SX3, DCS-7050X2 and DCS-7050X3 Series

- DirectFlow flows can be uninstalled from a linecard on reaching the idle timeout for the flow even though matching traffic continues to match the flow on another linecard. The flow can be restored by re-programming it or disabling the idle timeout.

  Series Affected: 7300X3 (411851)
  Series Affected: 7300X3, 7320X and DCS-7300X Series

- In an MLAG setup, under certain conditions, packets entering a LAG interface on one MLAG peer destined to the other peer might end up getting dropped on the MLAG peer link.

  A workaround for this is to restart the StrataLag agent. (412307)

- Hosts may incorrectly learn the ARP of virtual IP behind the switch MAC when the switch is reloaded or configuration is flapped.
  Workaround is to clear the ARP on the host to trigger a new ARP reply with the correct VARP MAC. (418626)

- Configuring more than 16K MPLS pop/swap labels will cause continuous restart of
  forwarding agent. (419243)

- Hitless Strata agent restart may cause a Port Channel interface to flap if it contains members with auto-negotiation speed configuration (419369)

- If the number of next-hop groups configured exceeds maximum supported hardware NHGs, then STRATA-3-MPLS_MAC_DA_PROFILE_TABLE_FULL syslog message is logged and L3 forwarding agent may continuously restart.

  The workaround is to scale down the number of next-hop groups configured to stop the agent from continuously restarting. (420234)

- Ethernet49-54 may not link up with peers over long copper cables.
  Workaround is to enable autoneg on both ends of the link with 'speed auto <speed>' command. (421121)
  SKUs Affected: DCS-7060SX2-48YC6-F and DCS-7060SX2-48YC6-R

- After a speed change, flows with mirroring actions on affected interfaces may not be mirrored as expected. Strata Slice agent can be restarted to restore expected behavior. (422221)
  Series Affected: CCS-720XP, DCS-7050SX3 and DCS-7260CX3 Series

- The forwarding agent may continuously restart if the speed is changed from 100G to 50G when a 50G QSFP transceiver is inserted.
  This only affects 2-lane 50G transceivers, and does not affect 100G transceivers operating in 50G mode.
  A workaround is to configure the speed before inserting the transceiver.
  The forwarding agent restarts can be stopped by temporarily configuring the affected interfaces in 25G mode. (424990)

- In scale policy-map configuration, in some cases, a config replace can lead to restart of Strata slice agent. (430654)
  Series Affected: DCS-7260CX Series

- During Leaf-SSU or SSO, interfaces with 100GBASE-SRBD transceivers may experience a single link flap. (440451)

- Hitless upgrade may fail if there are errdisabled interfaces.

  Workaround is to fix the speed misconfiguration to bring the interfaces out of errdisabled state. (445466)

- Changing Acl configuration rapidly and multiple times may cause the forwarding agent to repeatedly restart unexpectedly. (447584)

- Slice agent may restart unexpectedly on performing speed change and/or shutting/no shutting on a PFC enabled interface with traffic flowing out of the interface.

The issue will not be seen if PFC is not configured or traffic is not flowing. (462139)
  Series Affected: 7368 Series
  SKUs Affected: DCS-7060DX4-32-F and DCS-7060PX4-32-F

- Irregularities in processing of VXLAN SIP learning packets. (463138)
- Special filter is installed on MLAG port channel member interfaces to block packets ingressed from MLAG peer via peer link at egress to avoid loop. When the filter is not installed on a member interface before it is added to MLAG port channel, there might be a momentary loop when interfaces belonging to an
MLAG port channel link up. (471268)
- With PFC pause stream for lossless priorities on egress interface and data traffic destined to the egress interface for lossy and lossless priorities, few seconds of loss may be seen on lossy priority traffic on toggling PFC globally.
Workaround: Stopping PFC pause frames before toggling PFC globally. (477941)
- LANZ fabric thresholds may not be applied if the Strata slice forwarding agent restarts. Workaround is to remove and reapply the thresholds. (480422)
  SKUs Affected: DCS-7250QX-64-F, DCS-7250QX-64-R, DCS-7250QX-64-SSD-F, DCS-7250QX-64-SSD-R, DCS-7260CX-64-F, DCS-7260CX-64-R, DCS-7260CX-64-SSD-F, DCS-7260CX-64-SSD-R, DCS-7304, DCS-7308 and DCS-7316
- L3 agent restart or "reload fastboot" may cause routed packets to be misforwarded for up to 1 second. There is no workaround for this issue. (481604)
- Aggregate storm control rate limit is not honored for broadcast and multicast
traffic. (490511)
  Series Affected: DCS-7010, DCS-7050X, DCS-7050X2, DCS-7060X, DCS-7060X2, DCS-7250X, DCS-7260X3 and DCS-7300X Series
- If an MBA supplicant is not assigned a dynamic VLAN when it is authenticated on a port, and if the supplicant later moves to a new port which is in unauthorized state, MBA authentication on the new port will not succeed and the port will continue to stay in unauthorized state. (491230)
- In case of a Strata agent restart, an unshaped dynamic CoPP queue can end up being configured as a drop queue.

  The workaround is to reconfigure the dynamic CoPP queue. (493708)
- After a failed attempt to apply an ACL to an SVI, rollback to previous working config may leave the ACL in a state where it does not match expected traffic.

Reapplying the previous working ACL will correct the issue. (498355)

- Programming or updating a Router ACL may rarely result in forwarding plane slice agent restart and can leave the corresponding vlan permanently blocked. (498502)
- MLAG connectivity between the peers might go down after linecard OIR. Flapping MLAG peer-link interfaces will bring the MLAG connectivity back up (500162)
- When the control plane is down during SSU, ARP packets from the remote VTEPs may not be forwarded to edge members of the VLAN. There is no workaround to this issue. (501085)
- In some cases, post forwarding agent restart, egress ACLs may not work properly and can affect traffic egressing out of ports where this egress ACL is not applied
  Restarting the forwarding plane slice agent yet again will recover the system from the inconsistent state. (501088)
- With "switchport default phone vlan <vlan-id>" configuration, DHCP offer packets tagged with the default phone vlan tag might be sent out untagged on trunk ports (501749)
- It is possible that storm-control configuration will still be applied in hardware after removing the configuration. Workaround is to restart the Strata agent. (504901)
- Control plane traffic on routed or port-channel interfaces may be continuously blackholed. One or more forwarding agent restarts are required to recover, which causes all interfaces to flap and a brief traffic outage to occur. To restart the forwarding agent, execute "platform trident * reset" in the CLI enable mode. (512189)
- L3 routes with ECMP to multiple remote VTEPs may take longer time to converge when members in ECMP goes down. (513994)
- Interface default mtu may not apply properly on ports post reboot and cause IP fragmentation issues depending on packet mtu size. The workaround is to toggle the interface default mtu configuration. (515239)
- If a multi-ASIC linecard is hotswapped with a single-ASIC linecard in the same slot, the Snmp agent may continuously restart. The only workaround is to reload the system. (515667)
  Series Affected: 7300X3 and DCS-7300X Series
- Restarting Strata with an ACL config that doesn't fit in TCAM can leave system in an incorrect state where subsequent attempts to program ACLs can fail. (522674)

- 'deny any any log` MAC ACL rule will not drop DHCP traffic and DHCP traffic will still be snooped. (523037)
- Port security: protect mode will cease to function on an interface with Dot1x configuration when Dot1x is disabled globally.

  When Dot1x is disabled globally, Dot1x configuration should be removed from individual interfaces with port security: protect mode. (523664)
- Enabling per VLAN routing with an L3 interface that only has an IPV6 address will result in no routing of packets received on this L3 interface. Workaround is to flap the interface. (528490)
- During an SSO failover, interfaces with VXLAN configured may result in an increased traffic outage on the associated interface (528749)
  Series Affected: DCS-7300X Series
- Groups of four adjacent BASE-T ports share a common hardware resource; for example, Et1-Et4 and Et5-Et8 and so on. Due to an issue with the shared hardware resource, all 4 ports may fail to link up.

  On fixed systems, the workaround is to run `platform trident reset`. On modular systems, the workaround is to run `platform trident <linecard> reset` on the affected linecard. (529148)
  SKUs Affected: CCS-720XP-24Y6 and CCS-720XP-48Y6
- A mirror to GRE packet may incorrectly be tagged with a VLAN tag corresponding to the native VLAN if the next hop for the GRE tunnel is through a trunk port that is in an SVI. A workaround to this issue is making the GRE tunnel reachable through an access port if in an SVI or a routed port. (533903)
- Attaching a policer to class-default of an egress policy-map consisting of both IPV4 and IPV6 ACLs, is not supported and may lead to forwarding agent restart (534152)
- VXLAN encapsulated ARP request and reply packets that have more than one dot1q tag will not be properly forwarded. (535958)
- VXLAN encapsulated packets received with inner payload having more than one dot1q tag will result in outer dot1q tag being stripped when egressing out on a port. There is no workaround to this. (536312)
  Series Affected: CCS-720XP, DCS-7050CX3, DCS-7050SX3, DCS-7050TX3 and DCS-7050X3 Series
- Card may shutdown at temperatures below critical temperature threshold. (536948)
  SKUs Affected: 7368-4D, 7368-4P, DCS-7050TX3-48C8-F, DCS-7050TX3-48C8-R, DCS-7170-32C-F, DCS-7170-32C-M-F, DCS-7170-32C-M-R, DCS-7170-32C-R,

DCS-7170-32CD-F, DCS-7170-32CD-R, DCS-7170-64C-F, DCS-7170-64C-M-F, DCS-7170-64C-M-R and DCS-7170-64C-R

- When an MLAG peer is reloaded with VXLAN dynamic VLAN to VNI configuration, some VNI entries may not get programmed in hardware resulting in traffic outage.

  The workaround is to restart the StrataL2 agent. (549749)

- Changing the speed of a QSFP or SFP interface from 10G to 1G may cause a Strata forwarding agent restart under some circumstances. This will cause an interruption in traffic on all ports. Workaround is to change from 10G to another speed before changing to 1G. (550269)
  Series Affected: 7300X3, CCS-720XP, DCS-7050X3 and DCS-7260CX3 Series

- When using a config session that deletes and recreates an existing ACL applied to one or more SVIs, and detaches the ACL from its applied SVIs in the same config session, the affected SVIs may be left in a state that blocks all traffic.

  Reapplying the ACL to the affected SVIs will unblock them. Using "hardware access-list update default-result permit" will prevent blocking the SVIs during ACL modification. (555485)

- Deleting a PTP-enabled port channel while PTP is in Boundary mode and then disabling PTP with the 'ptp mode disabled' command may cause the member interfaces of the deleted port channel to fail to send some PTP packets if PTP is set back to Boundary mode with 'ptp mode boundary'. Disabling and re-enabling PTP on the affected interfaces or port channel containing the affected interfaces with 'no ptp enable' and 'ptp enable' will restore normal operation. (558065)

- QSFP subordinate port breakouts are not compatible with SSO and may result in extended traffic outage.

  Workaround is to cold boot the device with the correct speeds configured in the startup configuration. (558511)
  SKUs Affected: 7300X3-32C-LC and 7300X3-48YC4-LC

- Loop protect fails to detect loops on MLAG port channels. (559665)
  Series Affected: 7300X3, 7320X, CCS-720XP, DCS-7050CX3, DCS-7050SX3, DCS-7050TX3, DCS-7060CX, DCS-7060CX2, DCS-7060DX4, DCS-7060PX4, DCS-7060SX2, DCS-7260CX, DCS-7260CX3 and DCS-7260QX Series

- VXLAN rule in ACL applied on SVI will cause Strata slice agent to continuously restart. Workaround is to remove VXLAN rule from ACL applied on SVI. (559747)

- TCAM resource exhaustion can lead to VXLAN forwarding to fail.
  Workaround: Reduce TCAM resource utilization to allow VXLAN entries in TCAM by unconfiguring other features that occupy TCAM. (561231)

- When "show platform trident vxlan multihoming groups non-peering" is executed, StrataL3 agent may restart unexpectedly. (561420)

- Fabric interface on a linecard can sometimes end up in a state where it can discard all packets at egress.
  When this condition happens, the "show platform trident fabric counters queue detail" command will show that the drops increment while there is no increase in packets or bytes transmitted on the problematic fabric interface. To recover from the problem, it is necessary to restart the linecard forwarding plane agent by running "platform trident <linecard> reset". The recovery process can cause traffic disruption across several ports in the switch. (562860)
    SKUs Affected: DCS-7304 and DCS-7308

- VXLAN BUM traffic received on a MLAG peer link may violate split horizon checks and result in sending traffic back to the VXLAN fabric resulting in MAC flaps in remote VTEPs.
  Workaround is to flap the MLAG peer link port channel member that is affected. (567667)
    Series Affected: 7300X3, CCS-720XP, DCS-7050QX2, DCS-7050SX2, DCS-7050SX3, DCS-7050TX2, DCS-7050TX3, DCS-7050X2 and DCS-7050X3 Series

- The forwarding agent may incur an additional restart during the Stateful Switchover (SSO). This may lead to a brief traffic outage. Conditions include: any peer fabric interface down (visible through `show platform trident connections`) and fabric modules unplugged. (568323)
    Series Affected: 7300X3, 7320X and DCS-7300X Series

- Forwarding agent restarts, changing the forwarding table partition, or cold boots may result in the internal VLAN not being set on an interface.

  As a workaround, a manual restart of the StrataLag will fix this. (569584)

- Committing security access lists through CVP may restart forwarding plane slice agent. Post restart forwarding plane functionality will continue to work as is.
  Workaround is to use "hardware access-list update default-result permit" CLI. (571289)

- Strata forwarding agent may continuously restart when a PBR policy with an access list "permit vxlan" is applied on an interface. The workaround is to remove "permit vxlan" rule from the matching criteria. (576286)

- In a MLAG setup, non routable packets destined to VARP MAC address coming in on a VXLAN VLAN (either on VXLAN edge port or encapped and entering a

core port) can get looped over the peer-link. (577462)
  Series Affected: DCS-7250X and DCS-7300X Series

- If uRPF is configured only in one VRF, deletion of that VRF may disable routing for all VRFs configured on the device. (578952)

- If the slice agent is restarted with more than the maximum logical ports configured, port active state will not be guaranteed after the agent restarts. Ports that were previously active may become inactive and vice-versa.

  Workaround is to avoid configuring more than the maximum logical ports on a pipe. If the maximum logical ports must be exceeded, unexpected activeness changes can be avoided by preemptively restarting the slice agent using "platform trident reset". (580017)
  SKUs Affected: DCS-7050TX3-48C8

- Port channel(s) may not be programmed correctly under the following scenario:
  - port channels with interface members are configured
  - a new switch configuration is created where interface(s) is moved from one port channel to another
  - that new configuration is applied using the CLI "configure replace ..." or "copy ... running-config"

  Workaround options:
  - restart StrataLag agent using CLI "agent StrataLag terminate"
  - reload the switch (586414)

- Performing SSU may result in a cold reboot due to DMA cancellation failure resulting in extended traffic loss. (589308)
  SKUs Affected: DCS-7050SX-64, DCS-7050SX-64-F, DCS-7050SX-64-R, DCS-7050SX-64-SSD-F and DCS-7050SX-64-SSD-R

- When many VLANs and/or LAGs are configured, port channels may flap during SSU. (592390)

- DHCPv6 unicast packets which are not destined to switch are copied to CPU, which may forward the packet to destination along with one copy forwarded in hardware resulting in duplication of unicast DHCPv6 packets. (595070)

- A SSU reload may result in the SCD watchdog causing an extended traffic outage. (605183)

- In EVPN VXLAN setup with multicast routing enabled, ARP broadcast request and IPV6 neighbour solicitation packets may flood additional copies in the VLAN including a copy out the original source interface. (611692)
  Series Affected: CCS-720XP, DCS-7050CX3, DCS-7050QX2, DCS-7050SX3 and DCS-7050TX3 Series

- Changing the membership of an interface from port-channel A to port-channel B might result in no control-plane forwarding to/from pre-existing members of channel group B during stateful switchover. (611967)
  Series Affected: DCS-7300X Series

- QSFP transceivers inserted into a OSFP slot using OSFP-QSFP Adapter (OQA) after switch boot up will not link up.
  The workaround is to configure "shutdown" followed by "no shutdown" on all interfaces in the affected OSFP slot.
  Another workaround is to restart the forwarding agent using the CLI command "platform trident reset". This will lead to a brief traffic outage to occur on all ports. (612798)
  SKUs Affected: DCS-7060PX4-32

- ARP packets destined to VARP MAC on a L2 VLAN may get dropped instead of forwarding the packet on the VLAN. (613277)

- Routing of certain IPv6 prefixes may not work correctly when systems has one or more set of routes having following bit patterns. 1) Upper 96 bits are same and 2) Bits 65 to 96 has non-zero value. (614629)
  Series Affected: 7368, DCS-7060DX4 and DCS-7060PX4 Series

- Interfaces with 1000BASE-T SFP transceivers may report a false link up when configured with default, "no speed", "speed auto", or "speed auto 1000full". The workaround is to configure affected interfaces with "speed forced 1000full" instead. (614753)
  Series Affected: 7320X, DCS-7060CX, DCS-7060CX2, DCS-7060SX2 and DCS-7260CX Series

- MAC addresses might not age out on port-channels spanning across multiple chips (616314)
  SKUs Affected: CCS-720XP-96ZC2, CCS-720XP-96ZC2-F, DCS-7250QX-64, DCS-7250QX-64-F, DCS-7250QX-64-R, DCS-7250QX-64-SSD-F, DCS-7250QX-64-SSD-R, DCS-7260CX-64, DCS-7260CX-64-F, DCS-7260CX-64-R, DCS-7260CX-64-SSD-F, DCS-7260CX-64-SSD-R, DCS-7304 and DCS-7308

- When removing VARP MAC configuration, ARP replies destined to the previously configured VARP MAC will be consumed by the switch even when the configuration has already been removed.

  Workaround: Restart Strata agent or reload the device. (630505)

DCS-7010 Series

- 802.1x pause and guaranteed bandwidth cannot be configured at the same time. (91141)

- IPV6 traffic received over IPV4 tunnel interface may be dropped.

The workaround is to configure IPv6 address on all the ingress L3 underlay interfaces. (545486)

7320X, DCS-7060X and DCS-7260X Series

- A single event upset (SEU) in the IFP_TCAM_WIDE table may not be detected. This may cause traffic to be misclassified.

  A forwarding agent restart is required to forward traffic normally. (260334)

- If RPR or SSO is configured, Strata fabric agent restarts may cause switchover to occur. (368082)
  SKUs Affected: DCS-7304 and DCS-7308

- A single event upset (SEU) in the IFP_LOGICAL_TABLE_SELECT TCAM or IFP_TCAM_WIDE may not be detected. This may cause traffic to be misclassified.

  A forwarding agent restart is required to forward traffic normally. (383160)

- Packet buffer memory corruption can result in packets getting discarded without visibility in counters.
  When this condition occurs, the buffer usage reported by the "show platform trident mmu queue status" command exceeds the total number of buffers reported by the "show platform trident mmu buffers" command.
  A workaround is to run the "platform trident reset" command, which results in forwarding agent restart causing the links of the system to flap momentarily. (553299)

DCS-7260X3 Series

- Forwarding agent may restart when a 40GBASE-SRBD transceiver is inserted after the hitless reload. To work around, configure "speed forced 40gfull" on the desired interface prior to inserting the transceiver. (417311)

- A single event upset (SEU) in the TDM_CALENDAR* tables may lead to packet loss.

  A forwarding agent restart is required to forward traffic normally. (547328)

- Transceiver insertion or removal from a port used for recirculation in VXLAN routing may result in continuous traffic loss. Workaround is to flap the port by doing shut/no shut. on the interface. (590389)

- A single event upset (SEU) in the IFP_LOGICAL_TABLE_SELECT TCAM or IFP_TCAM_WIDE may not be detected. This may cause traffic to be misclassified.

  A forwarding agent restart is required to forward traffic normally. (625317)

7368 and DCS-7060X4 Series

- 802.3X pause is not supported (348758)
- MPLS traffic will be dropped if the nexthop MAC address ages out or not known.

  The workaround is to set the MAC address aging-time to a larger value or simply turn off MAC aging if possible. (389425)
- Link may be unstable at 400G with 400GBASE-DR4, 400GBASE-AR8 or 400GBASE-SR8 transceivers. (472927)
  SKUs Affected: 7368-4D and 7368-4P
- Control packets destined to link local IPv6 addresses may go to glean queue and hence could get dropped resulting in protocol flaps. There is no workaround to this issue. (475260)
- 100G-2 is not supported. (505274)
  SKUs Affected: 7368-16C
- Lossy traffic could be discarded at ingress interface instead of egress interface, if the ingress interface has "priority-flow-control mode on" configured. Because of this, the lossy priorities on the ingress port are vulnerable to head-of-line blocking. Buffer build-up on the lossy priorities is a necessary condition for the problem. (514254)
- OSPFV3 Control packets destined to the CPU may go to glean queue and hence could get dropped resulting in protocol flaps. There is no workaround to this issue. (520443)
- Speed change on a port-channel member can cause a flap in BFD and BGP sessions for the entire port-channel (520638)
- Issuing "show platform trident l3 shadow routes lpm" with large scale of routes may result in unexpected restart of StrataL3 forwarding agent. (523797)
- System may experience transient traffic drop on some of the existing routes, when new routes having some specific distribution are added to the system. (524510)
- Forward error correction cannot be disabled on interfaces with 100G auto-negotiation configured. (533108)
- Executing the CLI command "show platform trident l3 shadow l3-iif-profile" causes StrataL3 to unexpectedly restart. (582412)
- Changes in interface L1 configuration via CLI such as speed, forward error correction, or shutdown while traffic is running may cause an unexpected

forwarding agent restart. This will lead to a brief traffic outage on all ports. (595680)
Series Affected: DCS-7060X4 Series

DCS-7050X, DCS-7250X and DCS-7300X Series

- A port operating at 100Mbps with a 1000BASE-T SFP adapter may not transmit packets to its link partner or may transmit corrupt packets failing FCS checks at the link partner, even if it successfully links up.

  Workaround is to run a shut/no shut on the affected port. (80970)

- Configured as MLAG, link flap of one or more LAG peer-link member ports could cause brief flooding of packets over the peer-link and can also lead to double delivery of packets on the MLAG interfaces. (117870)

- (A1 silicon only) MPLS traffic gets incorrectly prioritized, causing other traffic on the same port to get dropped. (160269)
  SKUs Affected: DCS-7050QX-32

- Altering the priority of transmit queues of a port will result in some traffic loss on that port. (194460)

- A single-event upset (SEU) on the tables REPLICATION_FIFO_BANK* may not be corrected, which may lead to traffic loss. (391625)

- Sometimes, an interface can stop transmitting despite there being queued packets on the interface's egress queues. Doing a "shutdown" followed by "no shutdown" on the interface can resolve the problem. (400610)

- A single event upset (SEU) in the ES_PIPE* tables may lead to a forwarding agent restart, after which the switch forwards traffic normally. (547326)

- In the presence of large amount BUM traffic across several interfaces, discards may be observed on some CPU queues. (563505)

DCS-7050X2 Series

- When an interface which is transmitting at linerate is disabled and re-enabled, it might end up in a condition where it is unable to transmit any more packets. Disabling the interface again causes the Strata-FixedSystem agent to restart following which the interface continues to transmit properly. (245501)

- Packets sourced from an authenticated MAC on a Dot1X MBA authenticated port get punted to CPU. Unicast packets destined to authenticated MACs egress out tagged on a Dot1x MBA authenticated access port. Restarting StrataL2 will fix the issue. (532463)

- Vxlan multicast decapsulation will not work for packets that are sourced from unknown source VTEP. (538407)
- Continuous flapping of L3 interfaces could cause the StrataL3 forwarding agent to restart, resulting in a momentary traffic loss. (550872)
- When the per VLAN routing feature is enabled, it will drop existing BFD sessions and prevent new BFD sessions to the switch from getting established. (568298)

CCS-720XP Series

- With dot1x configured, ipv6 packets with hoplimit as 1 may not go to CPU affecting v6 BGP neighbourship. Workaround is to disable both v4 and v6 routing first, and then enable it. (525781)
- IPv6 BGP peering may not be formed due to HLIM=1 packets not reaching to CPU if
  - there is a speed change on any port,
  - there is a transceiver hot swap
  - IPv4/6 multicast routing is enabled.

  Workarounds:
  - Use HLIM>1 BGP packets by configuring `neighbor <IP Address> ebgp-multihop <hlim>` on the BGP peer.
  - Or if HLIM=1 packets are to be used, then for the first two cases turn off IPv4 and IPv6 unicast routing on all VRFs and then enable back again. There is no workaround for the third case. (563045)
- Setup with only Storm-control and scaled IP Locking configuration may cause slice agent to restart continuously. (599935)

DCS-7050X3 Series

- Hardware port resource (logical port) exhaustion may cause one of the following:
  - One or more interface to discard all packets.
  - Forwarding agent to restart (including continuous restarts).

  Hardware port resource exhaustion is identified by STRATA-4-HW_PORT_RESOURCE_FULL syslog. The switch may run out of hardware port resources (logical ports) in following cases:
  - Several 4x10G or 4x25G breakout ports are configured.
  - 40G-only transceivers inserted with a default speed configuration (e.g., 40GBASE-SRBD).

  The workaround is to reduce the number of 4x10G or 4x25G breakout connections to 2 (one breakout per following interface groups Ethernet49-52 and Ethernet53-56) and to configure 40G-only transceivers with the "speed

40g" interface configuration. After the configuration is applied, the forwarding agent must be restarted using the CLI command "platform trident reset". This will cause all interfaces to flap and a brief traffic outage to occur. (546409)

- Ports with inserted transceivers which only support 40G (such as 40GBASE-SRBD) and a default interface speed configuration may reserve 4 logical ports (hardware interface resources) instead of 1 on boot up. This may cause other interfaces to become inactive and the syslog STRATA-4-HW_PORT_RESOURCE_FULL to be logged.

  The workaround is to configure 40G-only transceivers with the "speed 40g" interface configuration. After the configuration is applied, the forwarding agent must be restarted using the CLI command "platform trident reset". This will cause all interfaces to flap and a brief traffic outage to occur. (554109)

- Interfaces may be unable to transmit or receive packets after the hitless reload or hitless restart of the forwarding agent, followed by interface speed change, or transceiver removal or insertion. An indication of the problem is the "inDiscards" in the output of "show interfaces counters discards". To recover, execute "platform trident reset". This command will cause all ports to flap and a traffic outage to occur. (570820)

Transceiver Series

- When performing an accelerated switch upgrade with the command reload fast-boot, some transceivers may experience a link interruption. This can occur on dual-speed QSFP100 optical modules that support both 100G and 40G, specifically when the module is configured to operate at 2x50G. Examples include the 100GBASE-PSM4 and the 100GBASE-CWDM4. (343684)

- Externally calibrated SFP form factor transceivers will operate with system default high alarm threshold of 63C and system default high warning threshold of 58C and may be logged as overheating when operating within their thresholds as programmed in the module EEPROM. (489787)

- Third party QSFP twinax cables may fail to initialize. This will result in them not showing up in 'show inventory'. Susceptible cables will have lower page 0 byte 2 bit 2 set to 0. This can be confirmed with the 'show idprom transceiver ethernet <intf> extended' while running an unaffected release. (556437)
  SKUs Affected: 100GBASE-CR4 and 40GBASE-CR4

- Removing a transceiver within approximately 3 seconds of inserting the same transceiver from a QSFP200, QSFP-DD or OSFP transceiver slot may cause XcvrAgent to unexpectedly restart. (569999)

- Egress ACL on SVI for BUM traffic will not match ACL rules for packets being sent across fabric interfaces. (284543)
- Tagged packets with any VLAN priority received through MLAG peer links are always mapped to the same egress queue, and not complying with "show qos map". (407056)
- Interfaces with certain types of optics do not come up after doing a administrative no-shut following a hitless reload operation if those interfaces were kept in admin down state prior to hitless reload. (416694)
- Interfaces with certain types of optics do not come up after doing a administrative no-shut following a hitless reload operation if those interfaces were kept in admin down state prior to hitless reload. (417223)
- If a hitless forwarding agent restart is attempted while the hardware configuration does not match the running configuration, then it may cause an additional forwarding agent restart and loss of traffic. This may also happen if the forwarding agent is restarted while some interfaces have been disabled due to insufficient logical ports. (417835)
  SKUs Affected: DCS-7050SX3-48YC8-F and DCS-7050SX3-48YC8-R
- Performing SSU may result in extended traffic outage, leading to total traffic loss being slightly over 1 second. (477139)
- Some NAT rules may not work correctly if the StrataL2 forwarding agent happens to restart. Packets may not get translated as expected
  The impacted rules need to be un-configured and then re-configured. (483821)
  Series Affected: DCS-7300X Series
- Aggregate storm control rate limit is not honored for traffic that is routed and flooded in the egress VLAN. (485492)
- If EVPN VXLAN multihoming is configured, and link towards ethernet-segment goes down, then some macs that reside behind that link may get stuck in hardware. As a result, traffic destined to those macs may get dropped. The workaround is to reboot the switch. (495546)
- Having any ACLs with UDF qualifiers as well as any of the following LAG/ECMP hashing features present in the configuration: RRoce hashing or TTL/HopLimit hashing, will result in incorrect operation of the LAG/ECMP hashing where the switch incorrectly hashes on IP payload. To avoid this problem the conflicting features should not be configured at the same time. (497016)
  Series Affected: DCS-7050CX3, DCS-7050SX3 and DCS-7300X Series
- If NAT configuration is modified or if a NAT-enabled interface is shutdown and enabled while traffic is flowing, then some of the NAT connections might

not be setup properly leading to packet loss or untranslated traffic.

Workaround is to be quiesce traffic before modifying the NAT configuration and then resume traffic. (497045)

- With VXLAN enabled, during SSO, control plane traffic make cause a kernel panic and unexpected reload on the new primary supervisor. (498652)
- With GRE tunnels or IPinIP tunnels or Nexthop-group tunnels configuration along with subinterface in the tunnel core interface, tunnel encapsulated packet will not be tagged with dot1q tag as configured in the subinterfaces, instead packet will go out tagged with internal vlanId assigned for the subinterface. There is no workaround for this issue other than removing subinterface configuration in the core interface. (523365)
  Series Affected: 7300X3, CCS-720XP and DCS-7050CX3 Series
- If MLAG peer gateway feature is enabled and MLAG peer link is configured as a port channel, it may result in Strata forwarding agent restart.
  As a workaround, peer link port channel has to be unconfigured and then restored. (523701)
- Link down events that causes VXLAN underlay ECMP shrink may result in traffic loss of more than 1 second. There is no workaround to this. (533790)
- Egress ACL rules can not be used to match ip protocol 50. (535104)
- SSU reloads from EOS releases in the 4.23 train starting with 4.23.2 version might fail with fatal errors or might leave the link interrupt functionality broken (537541)
  SKUs Affected: DCS-7050CX3-32S and DCS-7050SX3-48YC12
- Disabling static NAT access-list sharing with "no hardware nat static access-list resource sharing" may in some cases leak hardware VFP resources.

  Workaround is to reload the switch. (539951)
- In VXLAN setup, even with underlay ECMP configured, the traffic may not be hashed to all the ECMP links towards the spines. (540083)
- In a multi-homing setup, local-bias may not be honoured for unknown multicast traffic. This may lead to duplicate delivery of packets to the multi-homed host or packets may be looped back to the multi-homed source. (545462)
- Dynamic NAT access-list requires the subnets/hosts to be specified. It does not support ACL "permit ip any any".

  Possible workaround is to use deny ACL at the beginning to filter out traffic between private subnets and gateway that do not need translation. (546206)

- When Egress ip counter feature is enabled then running 'clear platform trident counters' command will cause slice agent to restart. System will recover after restart (546577)

- A single event upset (SEU) in the TDM_CALENDAR* tables may lead to packet loss.

  A forwarding agent restart is required to forward traffic normally. (547329)

- When the switch is reloaded with EVPN All Active config, the BUM traffic from some of the VTEPs may not be pruned correctly resulting in duplicate delivery of packets on some of the shared ethernet segments. The workaround is to restart the StrataL3 forwarding agent. (560034)

- When VXLAN IPv6 underlay is configured and when core interface is a port channel on a SVI, continuous port channel interface flaps may result in persistent loss of VXLAN traffic to remote VTEPs that are reachable through that port channel. (567455)

- VXLAN encapsulated packets received with inner payload having more than one dot1q tag will result in outer dot1q tag being stripped when egressing out on a port. (567587)
  Series Affected: 7300X3 Series
  SKUs Affected: CCS-720XP-96ZC2 and CCS-720XP-96ZC2-F

- During bootup or L3 agent restart, one or more linecards may not be programmed with all the routes. This will cause traffic loss or misforwarding. There is no workaround for this issue. (568757)
  SKUs Affected: 7300X3-32C-LC, CCS-720XP-96ZC2 and CCS-720XP-96ZC2-F

- VXLAN encapsulated packets with inner destination MAC as the switch MAC may get dropped when received on a L2 only VXLAN VLAN. (582895)

- When switching from EVPN configuration to static VXLAN, remote MACs may not be learned even though configuration is switched to dataplane learning.

  Workaround: Flap the VXLAN interface or restart StrataL3 agent. (596455)

- Performing SSU (fast reload) from an older release may lead to complete traffic loss. Workaround is to issue chip reset using "platform trident reset" command. (596509)

- Agent StrataL3 may not get properly initialised if segment security and multicast is enabled. Workaround is to disable these configurations and re-enable them one after another. (603915)

- On switch reboot/reload with NAT configured, the ports come up and then NAT configuration is applied. If traffic is flowing before the NAT configuration is fully programmed, then some packets might go out untranslated or dropped. Workaround is to stop traffic till NAT configuration is fully applied. (606202)

- When address-only NAT is configured, and after a host is assigned a NAT IP address, ACL check is skipped for subsequent flows from that host. Such flows gets translated even if they match deny ACL entry.

  Workaround is to use Dynamic NAPT or static NAT configuration. (613563)

- When two dynamic NAT connections are established with the same IPs on two different interfaces, the StrataNat agent may repeatedly restart.

  To resolve the issue, the device must be restarted. (613804)

- If dynamic NAT configuration is modified or if the interface configured with dynamic NAT flaps, NAT connections may be left untranslated.

  Workaround is to manually flush all the entries using the command "conntrack -F" in the corresponding network namespace bash mode. If configured on a non-default VRF (vrfName, for example), run the command "ip netns exec ns-vrfName conntrack -F". (615735)

- When address-only NAT is configured and the default NAT profile (NAPT) is configured, after a host is assigned a NAT IP address, ACL check is skipped for subsequent flows from that host. Such flows gets translated even if they match a deny ACL entry. (618773)

- If dynamic NAT rules with the same ACL are configured on more than 64 interfaces, the StrataNat agent may restart continuously.

  Workaround is to use different ACL names such that no more than 64 interfaces share the same ACL name. (621189)

- Restart of Forwarding plane agent renders a modular T3 switch blackholing the incoming traffic. A slice restart resolves the issue. (621224)

- Modifying the ACL configuration applied to the NAT rules with ECMP configuration is not supported.

  Workaround is remove the ACL, verify the rules are deleted from hardware and then re-apply the ACL. (623961)

- A single event upset (SEU) in the IFP_LOGICAL_TABLE_SELECT TCAM or IFP_TCAM_WIDE may not be detected. This may cause traffic to be misclassified.

  A forwarding agent restart is required to forward traffic normally. (626452)

DCS-7160 Series

- In some cases, when PFC (Priority Flow Control) is configured on an interface and if the user performs a "default interface" on a range of interfaces, the XpQos agent is restarted. (245559)

- In the event of the XpAcl agent restarting, the hardware programming of ACL may not be correct.

  In order to recover, remove the ACL configuration on ports/SVIs, and reattach them. (251114)

- On XP platforms, if XpMact agent restarts, and we have a large number of learned mac addresses and a large number of host routes, some of the host routes may get removed from hardware.

  To recover, clear all learned mac addresses and restart XpMact. (255279)

- VXLAN routing & bridging traffic may fail to converge after Sysdb agent is restarted.

  A workaround is to reboot the switch. (255957)

- In cases of high TCAM utilisation by Policy-based Routing, a 'configure replace' can result in Incorrect TCAM programming.
  In such cases, remove and re-apply the same policy-map which will result in programming the correct TCAM rules. (260906)
  Series Affected: DCS-7160 Series

- XPL3Unicast process may unexpectedly restart when the switch is reloaded if PBR policies with nexthop VRF actions are applied on an interface in the non-default VRF. (262713)

- IGMP IPv4 multicast control packets may create loop over a Vxlan Tunnel , if IGMP snooping is turned off in a VLAN. Workaround is to enable IGMP snooping in a VLAN (which is enabled by default in EOS) (429933)

- A sub-50 ms power outage may cause the links to go down permanently with the XpCentral agent crashing repeatedly. Reloading the system is required to recover from this failure. (457940)
  SKUs Affected: DCS-7160-48TC6-F and DCS-7160-48TC6-R

- Unexpected restart of the XpMact forwarding agent while there are unprogrammed MAC entries can cause some IPv4 and IPv6 unicast host routes to become unprogrammed. The fact that the routes are not programmed is only visible via "show platform xp ip(v6) route".

  A workaround for the inaccurate bookkeeping is to restart the XpL3Unicast forwarding agent. This will not reprogram the missing host routes.

  A workaround for the missing host routes is to reduce MAC scale and then restart the XpL3Unicast forwarding agent.

  To prevent this, configure "platform xp host-table dedicated" so that host entries cannot be overwritten by MAC entries. (552433)

Limitations and Restrictions in 4.24.2.9F

Accelerated System Update

- During a hitless reload upgrading from a release before 4.21.3, more than 3 LACP packets could be transmitted within a one second interval. This should not cause problems. (338048)
  SKUs Affected: DCS-7050SX-128-F, DCS-7050SX-128-R, DCS-7050SX-128-SSD-F, DCS-7050SX-128-SSD-R, DCS-7050SX-64-F, DCS-7050SX-64-R, DCS-7050SX-64-SSD-F, DCS-7050SX-64-SSD-R, DCS-7260CX3-64, DCS-7260CX3-64-F, DCS-7260CX3-64-R, DCS-7260CX3-64E-F and DCS-7260CX3-64E-R
- Aborting 'reload fast-boot' command with Ctrl-C is unsupported (344574)
- SSU of VRRP Master and Backup routers at the same time is unsupported and may cause extended traffic loss. Successfully SSU one router then SSU the other router. (345657)
- On systems with 4GB of /mnt/flash space, there may be insufficient space to store both an old swi image and a new swi image to perform an SSU upgrade. The workaround is to delete the old swi image from /mnt/flash prior to performing the upgrade. (385364)
- Performing SSU to boot into an image with this limitation may require that the currently running image is deleted to ensure that there is sufficient space available to perform the upgrade. (525870)

BGP EVPN L2/L3 VXLAN/MPLS

- On a BGP router, EVPN creates dynamic VLANs for L3 VNIs in receiving EVPN RT2 or RT5 advertisements even when the router does not have any L3 VRF or import route-target configurations. (294328)
- On a BGP EVPN device, if a VLAN-aware bundle is configured to include VLANs from multiple IP VRFs and if there are any IP addresses reused across multiple VRFs, then only one of the corresponding MAC/VLAN ARP bindings is distributed over EVPN. As a workaround, configure VLAN-aware bundles such that all VLANs in the bundle are in the same IP VRF. (514980)
- In an EVPN/VXLAN environment with VLAN-Based MAC-VRF, type 2 and type 3 routes are incorrectly imported when the route-targets match even if the VNIs are different.

  The workaround is to use different route-targets for the VLAN-Based MAC-VRF's to prevent the routes from being incorrectly imported. (631589)

CVX

- MapReduce Tracer is only recommended for deployments with 128 or fewer TaskTrackers.

  If a switch has more than 128 directly connected TaskTracker nodes with MapReduce Tracer deployed, then the MapReduceTracer Agent can increase CPU utilization significantly. It is recommended to keep the directly connected TaskTracker count to below 128 when MapReduce Tracer feature is deployed. (80403)

- When a new SDN controller with 'manager ip' command is configured in HSC, HSC retains the configurations (e.g., logical switches) received from the old controller.

  The workaround is to disable and re-enable the HSC service. (132171)

- Switches and CVX instances participating in a CVX setup must either all run 4.15.4F or later, or all run images from before 4.15.4F. (146664)

- If a CVX service agent connects to a client switch running a newer software version, the service agent may fail to connect to the client.

  Upgrade the CVX software to a version greater or equal to versions running on all client switches. (219403)

- Intercept hosts on trunk ports with native vlan are only supported on 7050X2 platforms (257580)

- The Macro-Segmentation Service (MSS), requires MLAG fast redirection be enabled on the service MLAG TOR pair, when configured to work with a L2 transparent FW. This configuration minimizes traffic loss when any individual interface in the MLAG port channel goes down. (268291)

- The MssClient agent, can restart unexpectedly, when the MacroSegmentation Service, deployed with a L2-transparent firewall and is configured to intercept more than 10,000 end-points on a single switch (a number that's far greater than the total number of intercepts possible on the switch). (283221)

- The MacroSegmentation Service (MSS) allows users to configure multiple tags on CVX that can be used in firewall policy definition, to identify policies MSS should work on. It is however not possible to delete one of the multiple tags configured.

  A workaround would be to remove all tags and reconfigure the subset required. (372320)

- In Macro-Segmentation Service (MSS) for L3 Firewalls , Virtual SVI IP addresses cannot be treated as intercepted hosts and thereby cannot be added to any redirect policy. However, these IPs can still be part of offload policies, even though implicit redirect will not work for them. (372504)

- If the Macro-Segmentation Service (MSS), working with a L3 firewall, is configured to intercept traffic from a host generating multicast traffic, the traffic can be black-holed.

  To work around this issue, configure the following DirectFlow rule on all TOR switches MSS is programming rules on and assign it the highest priority:

  ```
  flow bypassMulticast
     priority 65535
     table trident ifp
     match ethertype ip
     match destination ip 224.0.0.0 240.0.0.0
  ! (375156)
  ```

- MLAG devices in an environment with the Macro-Segmentation service (MSS) configured (with L3 firewalls), should have a high-priority DirectFlow rule configured to ignore traffic over the MLAG peer link. This can be configured using the following flow definition on each switch (assuming Po1 is the MLAG peer link):

  ```
  flow bypassPeerLink
        priority 65535
        table trident ifp
        match input interface Po1
        match ethertype ip (375185)
  ```

- The Macro-Segmentation service (MSS), running with L3 firewalls, requires the following flows to be configured on the service VTEP devices connected to the firewall manually in order to prevent return traffic from the firewall from being subject to MSS rules again. The flows required are:

  ```
  flow bypassFwIntf3
     priority 65535
     table trident ifp
     match input interface Po1103    >>>>>>>> lag interface connected to FW
     match ethertype ip
  !
  flow bypassFwIntf4
     priority 65535
     table trident ifp
     match input interface Et31    >>>>>>>> phy interface connected to FW
     match ethertype ip
  ! (375189)
  ```

- The MssPolicyMonitor agent might unexpectedly start running and eventually exit when the CVX functionality is disabled on the master CVX instance.

This does not have any side-effect on the operation of the Macro-Segmentation Service (MSS). (378077)

- When the Macro-Segmentation Service (MSS) is enabled and works with a L3 firewall, there can be a momentary traffic outage on reloading a MLAG peer if the CVX to VTEP (MLAG switch) connection is not re-established before the MLAG reload delay expires at the reloaded peer. (418560)
- If MSS policy enforcement rules configuration is changed from verbatim to group verbatim, the SandAcl agent can restart unexpectedly (433592)
- When Macro-Segmentation Service (MSS) is enabled on the CVX in an environment where no switch is configured as CVX client, multiple "excessive warmup delay" syslog messages for MssPolicyMonitor agent might be noticed. (497132)
- In a Macro-Segmentation Service (MSS) deployment with a PaloAlto firewall, enforcement policy configured with application using dynamic port assignment is not supported. (515749)
- In a Macro-Segmentation Service (MSS) deployment with a Palo-Alto firewall, a policy with multiple source or destination zones will be enforced over only one source zone and/or one destination zone.

  A workaround is to split the policy into multiple policies with single source and/or destination zone. An alternative is to add the source and destination subnets to the policy configuration. (567376)

General

- CLI does not allow access to files whose names contain spaces. (539)
- When VmTracer is used in a network that includes Cisco devices, ESX hosts connected to the Arista switch will see CDP frames from the Arista switch as well as from the other Cisco devices. VmTracer will display the VM info when the ESX host reports Arista's CDP info, but then will delete it when the ESX host reports other CDP info.

  The workaround is to drop all inbound CDP on all ports using MAC ACLs. (101756)
- EOS SDK-based applications must be run via the 'daemon' command configuration. They cannot be run directly from bash. (158431)
- EOS extension scripts and agents which do not use EOS-SDK will need to be modified to work in 4.16.6M and beyond. (158467)
- EOS swix extensions containing RPMs which were based out of or procured from Fedora distributions prior to Fedora 18 may fail to install due to

dependency issues. Suggested workaround is to recreate the swix files with the corresponding RPMs from Fedora 18 distribution. (162325)

- Packets with size greater than MTU of egress interface will not honor directflow flows and may not be forwarded (180927)
- SSO is hitful with subinterfaces. Protocols running on subinterfaces may experience session flaps during SSO. (188070)
- ACL drop counters cannot be cleared. (202905)
- when ACLs are configured with stats over port-channels, these stats are kept at the physical port level not at the port-channel level. (203131)
- With international and HW-REV-01 images and the introduction of "ip access-group <access-list name>" other configuration commands beginning with 'ip" that are configurable in the global config mode are not accessible in "router bgp" mode.

  To access those commands exit the "router bgp" config mode to switch to the global config mode. (219390)
- Changes made to running-config after a config session is created might be reverted when the config session is committed which contains changes in similar or related areas. Use 'show session-config diff' inside the config session before committing to verify what changes will be made. (226850)
- The uptime in the output of "show module" may not match the uptime as shown by "show version" or "show uptime". The uptime in "show module" represents the time the module has been up since the last change in the "Status" column in the output of "show module", which differs from the meaning of uptime in "show version" and "show uptime". (248230)
- To avoid interoperability problems when using strong SNMPv3 encryption algorithms, follow the following minimums:

  - When using AES192 for privacy, use a minimum of SHA224 for authentication.
  - When using AES256 for privacy, use a minimum of SHA256 for authentication. (268290)
- Copy commands with sftp: or scp: URL do not work via eAPI by passing password through the "input" parameter. SSH keys have to be setup to run the commands without a password. (283716)
- EOS support alphanumeric VLAN names, however ODL gives an error when reading the leaf /interfaces/interface/routed-vlan/config/vlan if the name contains alphabetic characters.

  To workaround use numeric VLAN names only in EOS. (361244)

- The Macro-Segmentation Service (MSS) fails to skips processing a tagged firewall policy if one of the interfaces in the zone are not configured with a valid IP for that zone.

  To workaround this problem, configure a valid IP address on the interface. (367835)

- Enabling next-hop sharing (using "ip hardware fib next-hop sharing" command) could result in slower convergence in the case of link failures. (369305)

- A reload with "The system rebooted due to a watchdog on the lower card" as the reload cause may occur unexpectedly on hardware built prior to 2020. (372163)
  SKUs Affected: DCS-7050SX-128-F, DCS-7050SX-128-R, DCS-7050SX-128-SSD-F, DCS-7050SX-128-SSD-R, DCS-7050TX-128-F, DCS-7050TX-128-R, DCS-7050TX-128-SSD-F, DCS-7050TX-128-SSD-R, DCS-7250QX-64-F, DCS-7250QX-64-R, DCS-7250QX-64-SSD-F, DCS-7250QX-64-SSD-R, DCS-7260CX-64-F, DCS-7260CX-64-R, DCS-7260CX-64-SSD-F, DCS-7260CX-64-SSD-R, DCS-7260QX-64-F, DCS-7260QX-64-R, DCS-7260QX-64-SSD-F, DCS-7260QX-64-SSD-R, DCS-7280CR-48-F, DCS-7280CR2-60-F, DCS-7280CR2A-60-F, DCS-7280CR2K-60-F, DCS-7280QR-C72-F, DCS-7280QR-C72-M-F, DCS-7280QR-C72-M-R and DCS-7280QR-C72-R

- For static tunnel interfaces, duplicate or conflicting GRE tunnels are tunnels that have the same source, destination, tunnel mode (GRE) and key configurations as an existing tunnel. A duplicate tunnel is always in the down state. When there are duplicate static tunnel interfaces and a config-replace is executed, it is non-deterministic which one of the conflicting tunnels will be in the up state. (373135)

- When an interface profile is used to configure an interface's access VLAN, the VLAN is not created automatically. The VLAN must be manually created with the vlan command. (376621)

- When using interface profiles, configuring interfaces may take a few minutes, depending on the number of interfaces being configured. It may be faster to apply an empty interface profile to the interfaces, and then update the profile. (382120)

- The CLI commands "locator-led [multifan | powersupply | chassis]" will not cause multifan, powersupply and chassis LEDs on the front panel of the system to flash, as they did on previous generations of fixed systems.
  The beacon LED on the back panel of the chassis is purple by default. The CLI commands "locator-led chassis" causes it glow red instead of expected blue. (395892)
  SKUs Affected: DCS-7050SX3-48YC8-F, DCS-7050SX3-48YC8-R, DCS-7280CR3-32D4-F, DCS-7280CR3-32D4-M-F, DCS-7280CR3-32P4-F, DCS-7280CR3-32P4-M-F, DCS-7280CR3-32P4-M-R, DCS-7280CR3-32P4-R, DCS-7280CR3K-32P4-F, DCS-7280PR3-24-F and DCS-7280PR3-24-M-F

- The configuration lock feature does not prevent changes to the configuration via SNMP. (402556)
- If an EOS CLI command is used to create a reference to a VRF that does not exist, a subsequent OpenConfig YANG operation may cause the VRF to be created in EOS. (411908)
- Large amounts of monitoring traffic processed at the control plane via aggressive sflow sampling or mirroring to CPU could affect other control plane functions due to CPU bandwidth contention. (415992)
- IP Locking may send out additional queries when STP changes state (even possible in portfast config which is common for the IPLocking use-case). (417806)
- When hardware or software flow tracking is enabled and tracking flow is a VXLAN flow, the exported IPFIX packet may contain incorrect inner VLAN ID. (421437)
  Series Affected: CCS-720XP Series
- When "logging format hostname ipv4" is configured, log messages may not display the correct IP address if the IP address is updated. (422666)
- In the 'show interfaces interactions' CLI, the list of speeds an interface is limited to does not account for the limitations that result from speed-group configuration. (434363)
- Configuring both TACACS+ and LDAP with SSL profiles and "fips restriction" may cause the Aaa agent to continuously restart. To use TACACS+ and LDAP with SSL profiles at the same time, remove "fips restriction" from the SSL profile configuration. (439333)
- Per-port denial of service protection (PDP) support has been removed. (440074)
- When we first configure a port-channel lag_type, we must set values for both aggregation/config/lag-type and ethernet/config/aggregate-id (i.e. member configuration) in the same transaction. The lag-type is populated in EOS once the port-channel has one member port and remains set. (445421)
- When eAPI is configured with invalid SSL profile, nginx will stop running and all http/s requests will be refused (474422)
- Currently EOS does not support parsing and separating multiple ACL rules in the same NAS-Filter-Rule AVP using zero byte delimiter. (475210)
- vlan A cannot be both source and target of 'floodset expand vlan' configuration at same time, i.e. have 'floodset expand vlan <vlan B>' and be used in 'floodset expand vlan <vlan A>' to configure vlan C (497773)

- Installed licenses without corresponding licensing features configured might not be visible from the CLI (504793)
- The YANG path '/network-instances/network-instance/mpls/global/config/null-label' is unsupported, but it is incorrectly listed as supported, and accepted by the OpenConfig agent. (514041)
- The following YANG paths are unsupported, but are incorrectly listed as supported and accepted by the OpenConfig agent.

  /network-instances/network-instance/policy-forwarding/policies/policy/rules/rule/action/config/decapsulate-gre
  /network-instances/network-instance/policy-forwarding/policies/policy/rules/rule/action/state/decapsulate-gre
  /network-instances/network-instance/policy-forwarding/policies/policy/rules/rule/action/config/discard
  /network-instances/network-instance/policy-forwarding/policies/policy/rules/rule/action/state/discard (515061)
- The following YANG paths are unsupported, but are incorrectly listed as supported and accepted by the OpenConfig agent.

  /network-instances/network-instance/segment-routing/te-policies/te-policy/candidate-paths/candidate-path/segment-lists/segment-list/sids/sid/state/mpls-tc
  /network-instances/network-instance/segment-routing/te-policies/te-policy/candidate-paths/candidate-path/segment-lists/segment-list/sids/sid/state/mpls-ttl (515063)
- If Octa, OpenConfig or TerminAttr are started under low memory conditions, they can cause a spike in CPU usage before unexpectedly restarting. (534841)
- When the "tunnel destination" address is configured as a broadcast address for static tunnel interfaces then there could be packets drops during decapsulation at the tunnel endpoint. (544032)
- For a given interface, multiple simultaneous MAC address flush requests on different VLANs may result in clearing all MAC addresses on that interface. This is an optimization to support a higher scale of VLANs and interfaces. To disable this optimization, use the "mac address-table flushing interface vlan aggregation disabled" CLI configuration. (544712)
- When running CLI command `show processes top`, or the "top" command via the bash shell, statistics about %CPU time are underestimated for most processes.
  To workaround this: use "top -b -n2" and ignore the first output (562245)
- Sampled flow tracking doesn't export proper bridging information (ingress VLAN, egress interface, egress VLAN, etc.) in IPFIX flow records for flows on

layer 2 subinterfaces when the bridging VLAN is different than the dot1q VLAN.
The workaround is to use the same dot1q VLAN and bridging VLAN for these layer 2 subinterfaces. (572688)

- When unsupported transceiver support is unlocked using a key, the ports that are in disabled state before unlocking will continue to be disabled.

  The workaround is to remove such transceivers and re-insert them after unlocking the unsupported transceiver support. (574146)

- Sampled flow tracking doesn't export proper routing information (VRF, next-hop, egress interface, BGP information etc.) in IPFIX flow records for flows on sub-interface with QinQ configuration. (575271)

- The 'logging level all' CLI expands to individual commands in the configuration, preventing dynamic updates of the logging list as part of EOS upgrades. (579047)

- TACACS+ authentication and authorization through SSH does not work with Pulse Secure server because EOS sends different port names in authentication ("ssh") and authorization (actual vty) requests which are rejected by the server. (583678)

- Sampled flow tracking exports IPFIX flow records with egress interface as 'discard' for flows on pseudowire patched interfaces. (603916)

- Power Loss wrongly recorded as the reload cause on this platform instead of the correct reload cause. (604561)
  SKUs Affected: DCS-7280CR3-32D4, DCS-7280CR3-32D4-F, DCS-7280CR3-32D4-M-F, DCS-7280CR3-32D4-M-R, DCS-7280CR3-32D4-R, DCS-7280CR3-32P4, DCS-7280CR3-32P4-F, DCS-7280CR3-32P4-M-F, DCS-7280CR3-32P4-M-R, DCS-7280CR3-32P4-R, DCS-7280CR3K-32D4, DCS-7280CR3K-32D4-F, DCS-7280CR3K-32D4-R, DCS-7280CR3K-32P4, DCS-7280CR3K-32P4-F, DCS-7280CR3K-32P4-R, DCS-7280CR3MK-32D4, DCS-7280CR3MK-32D4-F, DCS-7280CR3MK-32D4-R, DCS-7280CR3MK-32P4, DCS-7280CR3MK-32P4-F and DCS-7280CR3MK-32P4-R

Layer 1

- The MACSec outPktsEncrypted and outOctetsEncrypted counters are not supported with the MACSEC Proxy feature (281715)

- On Vxlan MACsec proxy, disable learning is not supported on proxy patch vlan. (284348)
  SKUs Affected: 7500R2M-36CQ-LC, DCS-7280CR2M-30-F, DCS-7280SRAM-48C6, DCS-7280SRAM-48C6-F, DCS-7280SRAM-48C6-R, DCS-7280SRM-40CX2-F and DCS-7280SRM-40CX2-R

- Ports configured at PAM4 speeds (50G-1, 100G-2, 200G-4, 400G-8) do not support link-debounce intervals shorter than 2 seconds. (500674)
  Series Affected: 7368 and DCS-7060X4 Series
  SKUs Affected: DCS-7280CR3-32D4-F, DCS-7280CR3-32D4-M-F, DCS-7280CR3-32D4-M-R, DCS-7280CR3-32D4-R, DCS-7280CR3-32P4-F, DCS-7280CR3-32P4-M-F, DCS-7280CR3-32P4-M-R, DCS-7280CR3-32P4-R, DCS-7280CR3-96-F, DCS-7280CR3K-32D4-F, DCS-7280CR3K-32D4-R, DCS-7280CR3K-32P4-F, DCS-7280CR3K-32P4-R, DCS-7280CR3K-96-F, DCS-7280CR3MK-32D4-F, DCS-7280CR3MK-32D4-R, DCS-7280CR3MK-32P4-F and DCS-7280CR3MK-32P4-R

- Interfaces with BCM82391 PHY do not support auto-negotiation. (537530)
  SKUs Affected: 7500RM-36CQ-LC and DCS-7050CX3M-32S

Layer 2

- LACP PDU fast rate ("lacp rate fast" on an Arista switch) should not be configured on any port in an MLAG pair, or any port connected to an MLAG pair. (13950)

- Static ARP inspection may not work on modular platforms after SSO switchover. The workaround is to disable and re-enable static ARP inspection after switchover. (244477)

- The command "lacp rate fast" is not supported on modular systems with stateful supervisor switchover (SSO) enabled. Neighboring devices should not have "lacp rate fast" configured on ports connected to the said system. (248121)

- In a MACsec profile, when a primary key's CKN is changed, then operating primary continues to be principal actor even when a fallback key is configured till the time the new primary establishes a successful MKA session. There is zero traffic disruption. (275678)

- Port Security Protect does not support trunk ports. If a port is secured to source MAC <A> in VLAN <X>, traffic from source MAC <A> in other VLANs of the trunk port will also be allowed. (344773)

- While performing SSO, a device's peers might not receive LLDP packets within default TTL (120 seconds) and those peer devices may not maintain LLDP status information for the device undergoing SSO. After SSO is complete, the peers will again have LLDP state available.

  To avoid losing LLDP state during SSO, consider increasing LLDP hold time at the remote. (347459)

- If 'traffic unprotected allow' is configured in a Macsec profile, agent restart or Stateful Switchover may result in traffic loss (362766)

- An MLAG switch cannot be used as an EVPN multi-homing provider edge. When a switch has MLAG enabled, MAC addresses from ports with an ethernet segment configured are advertised through BGP as if they were single-homing, and local ethernet segments are not advertised through BGP. (397867)
- Even with fallback to unprotected traffic configured, traffic loss in the order of milliseconds may be seen during initialization (491232)
- Upon programming a large number (~250) of VTEPs in a flood set at once, the L2Rib agent may restart. Workaround is to program them in batches, waiting a few seconds between each batch. (544051)
- 802.1X is supported on LAG member ports using EAPOL authentication. (544556)

Layer 3

- ECMP is not supported for routes learned via RIP. (34773)
- DHCP relay is not supported when running virtual machines on EOS (101754)
- CLI does not detect TCAM exhaustion and automatically revert the change when a PBR policy is applied to an L3 interface in the "shutdown" state, since the actual hardware programming happens when the interface comes up. (122651)
- OSPFv3 support for multiple address families (RFC 5838) in EOS introduces support for IPv4 routing with OSPFv3. OSPFv3 for IPv4 AF in EOS requires configuring neighboring OSPFv3 IPv4 routers on the same link with primary IPv4
  addresses in the same subnet. Adjacency is established in OSPFv3 IPv4 AF even if
  the neighbor's primary IPv4 address is in a different subnet but routes through
  the neighbor on a different subnet will however not be installed. This limitation may be removed in a future release. (140234)
- When BFD is unconfigured with Fhrp as the only client and/or BFD is administratively shut, both VRRP routers will become Master. This transition is
  temporary and Master-Backup relationship will be restored. (159647)
- BFD sessions established between Arista switches and Cisco peers over IPv6 link-local addresses may flap when BFD echo mode is enabled. (159803)
- vEOS does not support BFD echo sessions. (160770)
- If "bfd per-link rfc-7130" is configured on port-channel(s) with primary and secondary IPv4 addresses configured in the same subnet, and the "bfd neighbor" is configured with peer switch port-channel's secondary IP address and there is a BFD session using primary IP address, then the port-channel

might flap continuously.

Configure secondary IP address on the affected port-channel(s) to different subnet from their primary IP address on both switches. (182622)

- BFD echo functionality is not available on L2 Port-Channels with BFD RFC7130 mode enabled. (190418)
- If a port channel is configured with "bfd echo" and "bfd per-link rfc-7130" and is used for OSPFv3 or PIM, BFD sessions will not come up with echo functionality. BFD with SSO for OSPFv3 or PIM is not supported. (190997)
- SSO is not supported when BFD is configured for ISIS IPv6 sessions. (239704)
- An LACP port channel configured with BFD per-link and echo may experience BFD session flap on existing member links if new member link(s) are added to the port channel while the BFD peer device undergoes Stateful Switchover (SSO). (255042)
- Eos does not support programming IPv6 ECMP paths to kernel (258387)
- The DSCP value of BGP control plane packets set by the command 'bgp transport qos
  dscp <value>' will be overwritten when the platform 'qos rewrite dscp' is enabled
  and the outgoing interface is a SVI based on traffic-class to dscp map present on
  the platform. (269764)
- In the output of the "show ipv6 dhcp relay counters" or "show ip dhcp relay counters" command, interface-specific DHCP relay counters might not sum up to "All Req" and "All Resp" counters. (278786)
- Tunnel interfaces flap when configuring ttl, tos and path mtu discovery on them. (281464)
- IPv6 addresses are not supported as tunnel source and destination. (283912)
- High MPLS route scale or high MPLS route churn may cause the platform agent to restart unexpectedly. (289217)
- High MPLS route scale or high MPLS route churn may cause the platform agent to restart unexpectedly. (289224)
- When BFD is configured with per-link mode rfc-7130 for an IPv6 link-local address on a Port-Channel and the Port-Channel transitions to the Down state, the Port-channel may not transition back to the UP state.

  The workaround for this situation is to disable and then re-enable BFD per-link mode rfc-7130 on the Port-Channel. (343814)

- On Macro-Segmentation Service (MSS) deployment with L3 firewalls, a flow entry that fail to get programmed due to lack of TCAM space, is not programmed when TCAM space becomes available at a later time. The workaround is to "shut" and "no shut" on the direct flow config. (372232)
  Series Affected: DCS-7050TX, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060X and DCS-7060X2 Series
- The update wait-install feature may not work as expected if there are routes which fail programming due to hardware resource exhaustion. The routes which failed programming may still get advertised out to peers. (372765)
- DHCP packets will not be processed by EOS DHCP Server when DHCP Relay is relaying packet from one SVI where DHCP Relay is configured to another SVI where DHCP Server is configured. (389017)
- When a sampled packet egresses a trunk port and the path is ECMP, sFlow will arbitrarily pick one of the ECMP next hops for the next hop IP of the router extension. (415747)
- DHCP clients will fail to obtain IPv6 leases when "ipv6 dhcp relay destination" is set to IPv6 multicast address. (426796)
- Destination (TEP) or include hop entry for a RSVP tunnel can be TE router ID of a
  router or IP address on any interface that has an IGP neighbor. It cannot be any
  other interface address, like a loopback interface address which is not TE router ID
  or a stub interface address. (453019)
- Nexthop group tunnel counters does not work, when tunnel counters is enabled using 'hardware counter feature mpls tunnel' command. (474078)
- VXLAN features are not compatible the 'ip hardware fib next-hop sharing' configuration. Configuring VXLAN routes may result in identical FECs not being shared and potential misforwarding after changes to FECs are made. (477471)
- The config 'ip hardware fib next-hop multi-path maximum' does not restrict the size of installed next-hop group ECMP FECs (498484)
- CLI configuration of a static route with nexthop pointing to self ip address is not rejected. (514894)
- New NAT dynamic profiles might lead to undefined behavior upon reload. (521178)
  SKUs Affected: DCS-7050SX3-96YC8, DCS-7050SX3-96YC8-F and DCS-7050SX3-96YC8-R

- NAT dynamic profiles are not supported on multi-chip and modular system. (525213)
  Series Affected: 7300X3, CCS-720XP and DCS-7300X Series
- BFD over Vxlan does not work for IPv6 underlay. (526897)
- Rsvp autobandwidth feature does not work for single hop tunnels. The workaround
  is to configure Rsvp explicit-null on the egress router for single hop tunnels. (571177)
- VARP VTEP IP configuration is not supported on AP aggregation VTEPs

  It is recommended that either EVPN VXLAN symmetric or asymmetric IRB be used for distributed VXLAN routing in campus environments. (571517)
- IS-IS Extended administrative group (EAG) sub-TLV is not supported. If a system in the network advertises EAG, Arista router will ignore the sub-TLV. (628807)

Multi-agent

- If a BGP peer is configured for BFD fallover, the BFD session is not cleaned up even after the BGP peer is unconfigured. (217199)
- Traffic destined to an L3EVPN route whose underlay has ECMP BGP-LU routes, may experience temporary traffic loss when the underlay goes from n way to n-1 way or lower. The duration of loss can vary depending on the scale of BGP-LU routes or L3EVPN routes. (251692)
- When the multi-agent routing protocol model is configured, the maximum number of next hops for an OSPF ECMP route is 128. (274888)
- With very a very low multi-hop BFD timer configured, a BFD session may flap when a path (belonging to an ECMP set), over which the BFD session is established, goes down. (287571)
- Route-map specified as match-map for dynamic prefix-list is evaluated only against BGP routes. (345444)
- The IpRib agent runs out of addressable memory when a large number of routes are leaked to a large number of VRFs. (346575)
- Routes which are imported into a target VRF using a "leak routes source-vrf" policy cannot be matched on the basis of the source-protocol from the source-VRF as part of the "rib fib policy" (403739)
- In multi-agent mode, extended Sflow BGP data is not supported for BGP LU routes. (411762)

- When using 64-bit versions of EOS, Bgp, BgpCliHelper and Bmp agents may report a virtual memory size up to 50 GB larger than actual memory used. The actual memory usage is better represented by the sum of "RES" and "SHR" from "show processes top". (427364)
- When BGP router has advertised a large scale of routes (e.g. several million) and it reloads, there may be traffic drops while it is coming back up. This happens when the reloading router comes back up before the directly connected peering routers (which are receiving routes via an intermediate Route Reflector) get a chance to process millions of withdrawals and delete all the routes from FIB. (458127)
- An AS_PATH prepend operation in an RCF function applied towards an IBGP peer is ignored. (474006)
- RCF compiler does not accept all characters allowed in prefix list names, community list names, and AS path list names. (483676)
- When a router receives a BGP route with an AIGP metric attribute value approaching 64-bit unsigned integer maximum value, another BGP route with a next hop covered by the first BGP route may not have it's MED attribute correctly advertised should it match an outbound route-map policy with 'set metric igp next-hop-cost' configured (487359)
- IP ACLs are not supported for control plane route filtering for VRF leaking (536329)
- Matching on origin-as validity in an outbound route-map has no effect. (547796)
- Match dynamic prefix-list clauses in route maps are only supported for BGP inbound and outbound route maps. (564552)
- BMP, SNMP and EosSdk will not report multiple BGP peers configured with the same BGP peering address. (602657)

Rib

- No support for IPv6 labeled Unicast capability when BGP neighbor is established using IPv4 transport. (208402)
- Match dynamic prefix-list clauses in route maps are only supported for BGP inbound and outbound route maps. (261865)
- Dynamic prefix-list match clauses are not supported in BGP neighbor inbound route maps. (269663)
- The BGP configuration commands, "bgp next-hop-unchanged" and "neighbor next-hop-unchanged", are not supported in ribd mode (single-agent mode).

In ribd mode, this functionality can only be achieved via route map configuration. (275007)

MLAG

- Spanning-tree mode backup does not work in an MLAG configuration. (15151)
- The port-channel configured on each MLAG switch with the same MLAG ID must also have the same channel-group ID. (22890)
- Configuring a device connected to an MLAG with a round-robin LAG distribution algorithm is not supported if the device is going to participate in IGMP. (28370)
- On a scaled MLAG setup, Lag+LacpAgent agent may restart unexpectedly if MLAG is reinitialized due to configuration changes. (116125)
- On an MLAG system configured with dual primary detection and with default control plane ACL enforced, MLAG will not form if the management interfaces of the MLAG peers are connected through extra hops (e.g., on different subnets), due to the default control plane ACL dropping MLAG control packets with TTL < 255.

  The work around is to apply a control plane ACL which permits MLAG control packets with the correct TTL. (271308)
- TCAM profile switch in a MLAG switch may result in some packet duplication for broadcast or multicast packets (341353)

MPLS

- The MPLS agent may continuously restart on a router with high BGP LU Tunnel scale. (377939)
- BGP LU Tx MPLS routes corresponding to BGP LU advertisements with multiple labels are not supported. (395029)
- MPLS vias in the LFIB are limited to 128 even when the maximum allowed ECMP or UCMP values exceed this number (602879)

Multicast

- If a single IGMP snooping port has multiple multicast hosts attached and performs proxy reporting or report suppression from these multiple hosts downstream, immediate-leave must be disabled for the VLAN.

  Use "no ip igmp snooping VLAN <vlanId> immediate-leave". Otherwise, some desired multicast traffic might be lost. (21367)

- After ASU reload, if the first PIM hello packet received from the neighbor gets lost and If the neighbor has a high hello query-interval, it will result in traffic loss. Workaround is to use default PIM hello query-interval and increase the PIM hello query-count. (341447)
- With scale greater than 5000 multicast IPV6 routes, show platform sfe mroute ipv6 <vrf> commands might not display the right number of routes when performing multiple addition/deletion operations across VRFs. This is applicable only if user level multicast forwarding agent is configured to be used instead of kernel. (378841)
- Bessd might unexpectedly restart on config replace with scaled setup over 30 VRFs and large number of PIM enabled interfaces. Work around is to reduce the scale. (398185)
- Pim "non-dr install-oifs" feature becomes disabled if the non-dr needs to route multicast traffic for any reason to the interface on which the feature was originally configured. This is how the feature is expected to work. The workaround is to setup the network in a way that the DR always becomes the assert-winner. However, if the non-DR becomes assert winner for some routes on an interface and feature becomes disabled, flap the pim sparse mode configuration on non-DR on that interface to attempt to get out assert winner state. (401672)
- Multicast routes are not created when a source is transmitting only fragemented multicast packets.
  Switch to using SFE for multicast software forwarding. (605326)

SwitchApp

- IGMP snooping filters are not supported when SwitchApp over forwards IGMP reports. Reports are over forwarded if the "igmp flooding" CLI is enabled through the FPGA instance CLI, or if the FPGA profile does not support correct forwarding of IGMP reports. (601917)

vEOS Router / CloudEOS

- The /mnt/flash/cloud_ha_config.json based configuration for the CloudHa agent is not supported from this release. If you are upgrading from an older image (< 4.20.5) please reconfigure HA using EOS CLI.
  Please see information on converting json file based config to CLI commands in the vEOS Router Configuration Guide. (264660)
- While vEOS instances in an AWS cloud can be created using either a Bring Your Own License (BYOL) or Pay As You Go (PAYG) format, there currently is no show command in vEOS to easily help the user or support determine which mode this instance uses. (272649)

- Tx/Rx ring parameters of an "Elastic Network Adapter (ENA)" interface cannot be set through config.json in vEOS. (276382)
- vEOS supports up a maximum of 8 physical cores. With hyperthreading enabled it is 16 vCPUs (278286)
- In dpdk based vEOS(MODE=sfe in /mnt/flash/veos-config), SR-IOV mode doesn't work with Intel x520/82599 on ESXi. As a workaround use mixed mode instead of the SRIOV only mode in ESXi (296718)
- Hot detaching network interface instances is unsupported. Reboot the instance after detaching a network interface. (306132)
- Site-to-site path monitored under "router path-selection" may experience flapping, when a lot of packets on the path (>10%) are dropped due to too much traffic injection into the virtual router. Workaround is to use QoS service policy to assign Inband Telemtry control packets (default UDP destination port is 4789) with a higher priority. (434087)
- CloudEOS does not support more than 10k /30 routes. The SFE agent will restart if more than 10k /30 routes are added to the system. The workaround is to reduce the number of /30 prefixes. (540204)

DCS-7170 Series

- If an ingress packet contains more than one 802.1Q tag and the egress port is a trunk port, the egressing packet may get corrupted. (180436)
  Series Affected: DCS-7170 Series
- Changing port speed from 10G/25G/50G to 40G/100G will cause the forwarding agent (BfnSliceAgent) to restart. This can result in a brief traffic outage in the order of 100ms on all ports. The link state of other ports will not change. (256519)
- 10/25/50 Gbps interfaces only support MTU up tp 7Kbytes. (258823)
- After applying or removing shaping configuration on an L2 sub-interface, the L2 sub-interface must be flapped for the configuration to take effect. (281312)
  Series Affected: DCS-7170 Series
- After setting CoPP rate = 0, a few packets (<10) might be let into the CPU, but everything will be dropped afterwards. (350676)
- Full mroute scale may not be achievable under certain scenarios due to hash collision for the multicast route table. (380545)
- When egress NAT and MLAG are both used, 'show ip mroute' may show NAT'ed addresses in addition to the receiving mroute addresses. (394571)
- firewall profile on DCS-7170 platform does not support IP multicast (401134)

- VXLAN encapsulated ieee reserved mac addresses are not trapped to CPU and hence
  any control protocol that is VXLAN encapsulated will not work. (423963)

- Accelerated Software Upgrade (ASU) is not supported in combination with the packet-filter profile. The hitless reload will time out and fall back to a normal reload. (473985)
  Series Affected: DCS-7170 Series

- On the DCS-7170 series, ASU is not supported on the firewall profile. (475112)
  Series Affected: DCS-7170 Series

- Hitless reload may incur several seconds of traffic outage if route scale is large (490931)

DCS-7170 Series

- On the 7170 series of switches, when IPv6 in used in VXLAN underlay, the UDP checksum
  will be 0 for all the packets going out with an IPv6 VXLAN encapsulation. (297660)

CCS-720XP Series

- "show environment power" does not show insertion status or telemetry information for PWR-1021-AC-RED or PWR-621-AC-RED when there is no input power. (369368)
  SKUs Affected: PWR-1021-AC-RED and PWR-621-AC-RED

- When hardware flow tracking is enabled, tcpControlBits information element in IPFIX flow records for VXLAN encapsulated TCP flows is incorrect. (416079)

- On receiving COA-REQ for changing VLAN for EAPOL supplicant, the NAS deliberately fails authorization for the first time in the new vlan. (449890)

- The per-interface configuration to ignore reauthorization timeouts from the AAA server ("dot1x timeout reauth-timeout-ignore") is not designed to work if manual reauthorization is requested from the command line. The reason for this is that manual reauthentication is designed to force the supplicant to contact the AAA server to retrieve the latest credentials. (453044)

- CoA request for VLAN change for EAPOL supplicant returns CoA-NAK. The VLAN does get changed when device is reauthenticated and the AAA server sends the new VLAN in an Access-Accept response. (459726)

- Hitless FPGA upgrades are not supported due to hardware limitations. Therefore FPGA images will not be upgraded during SSU. (474978)

SKUs Affected: CCS-720XP-24Y6-F, CCS-720XP-24Y6-R, CCS-720XP-24ZY4-F, CCS-720XP-48Y6-F, CCS-720XP-48Y6-R and CCS-720XP-48ZC2-F

- Negation operator (!) and 'assigned' keyword are not supported in Radius NAS-Filter-rule(attribute-id 92) Attribute. (475207)
- Ip options qualifiers are not supported in the NAS-FILTER-RULE attribute if present in the Access-Accept or COA packet from the AAA server. If Ip options are present in NAS-FILTER-RULE, it may cause supplicant to fail authorization. (480659)
- WOL feature is currently only available for phone trunk port, but not for regular trunk port. (481468)
- Fallback to MBA authentication feature may not work as expected with Caching Auth feature. (482333)
- Timeout value configured for MBA fallback feature can block MBA Auth for upto 60 seconds more than the configured value since first non-EAPOL packet is received. It is recommended to configure the hold period to be lower than the timeout value for MBA fallback. (483995)
- MBA for passive device can not be triggered by ARP/ICMP if IP locking is enabled (500439)
- If a switchport loses power, the credentials of the attached phone and PC will
  remain cached when authentication caching is enabled. However, when power is
  restored, the EAPOL enabled PC may not be reachable within the default reauthorization limit of 3 attempts and the supplicant will be removed as a result.
  The solution in this situation is to increase the reauthorization limit using the
  per-interface dot1x command: dot1x reauthorization request limit 10 (500488)
- Limitation - 802.1X Web Authentication Implicit ACL feature doesn't work when IP Locking is configured on the interface. The workaround is to use 802.1X ACL based Web Authentication. (557986)

DCS-7160, DCS-7170, DCS-7280R and DCS-7280R2 Series

- On devices with Algomatch enabled, removing an ACL on an interface might fail because the remaining ACLs on the system may not fit in the hardware tables. (192811)
- Ingress ACLs on IPv6 packets do not work when IPv6 uRPF is configured and AlgoMatch is enabled. (512394)

7368, DCS-7300X, DCS-7500R and DCS-7800 Series

- BFD on a statically-configured port channel may flap and traffic may be lost on a linecard insertion of which an interface is a member of the port channel.

  Use LACP or disable the port-channel members on the inserting linecard before the linecard insertion (361336)

- Non per-link BFD sessions over port-channels may flap when a linecard where some of
  the port-channel's members reside is powered off with "no power enable". (363122)

- When a system shuts down due to a power overload, EOS does not log a 'power overload' reload cause (371160)

- Mixed supervisor types are not supported on dual-supervisor modular systems. (450053)

- With scaled VRF, SVI and Arp entries, typically beyond claimed support, the Arp agent may experience a SIGQUIT during SSO switchover, on the new active supervisor. There is no workaround for this issue and switchover is ultimately successful. (495528)

- When 1000 VRFs are configured with 4000 SVIs, the Ira agent may experience a SIGQUIT during SSO switchover. There is no workaround for this issue and switchover is ultimately successful. (495529)

CCS-720XP Series

- Polycom SoundStation IP 7000 phone might stop sending traffic after a switch power cycle if the phone stays on PoE power without an L1 link for some time.

  Workaround is to toggle PoE power on the affected interfaces with "poe disabled" followed by "no poe disabled". (502688)

- When 'poe shutdown action power-off' CLI config is in use, PoE power will not be turned off when an interface is errdisabled (506677)

DCS-7020, DCS-7280R, DCS-7280R2, DCS-7280R3, DCS-7500R, DCS-7500R2, DCS-7500R3 and DCS-7800R3 Series

- The L3 MTU on interfaces is not enforced on SVIs. (11659)
  Series Affected: DCS-7020, DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series

- Disabling IPv6 routing on an L3 interface is not supported when IPv4 routing is also enabled on that L3 interface. (43093)
- show interfaces counters rates' for port channels may show a slightly inaccurate data rate (including above 100%). (67367)
- A VXLAN encapsulated packet after de-encapsulation is not forwarded back to the port on which the original packet was received.
  Similarly, a native ethernet packet after VXLAN encapsulation is not forwarded back to the original receive port towards the remote VTEP. (75075)
- VARP and VRRP cannot be enabled at the same time. If VRRP is configured, there can be up to 128 combinations of interface and Virtual Router ID (VRID), but there can only be at most 8 different VRIDs and the VRIDs must differ only in the 3 least significant bits. VRRP for IPv4 and IPv6 cannot be configured at the same time. (75752)
- Due to hardware limitation, if an egress IP ACL is applied on an interface which is part of a VLAN with an egress router ACL, the filtering behavior for egress traffic of that interface may be undefined. (82094)
- For packets that hit rules across multiple ACLs, the hit counts are accounted for only in a single ACL. PACL counters take precedence over RACLs and MAC ACLs, and RACL counters take precedence over MAC ACLs. (85440)
- When an egress IPv6 RACL is applied to a VLAN, IPv6 packets may not be subjected to MTU checks. (88778)
- An egress ACL on a destination port of a monitor session only takes effect for Rx mirrored packets which are IP forwarded. The egress ACL will not work for bridged packets or Tx mirrored routed packets. (89915)
- When a shaper is configured the output of the shaper has a tolerance of +30% with 100-byte frames. This reduces to +5% as the frame size is increased to 600 bytes. The shaper variance reduces when the port happens to be the endpoint of a tunnel. (93546)
- The egress per-queue byte counter is not exact for certain packet types. For routed packets the egress per-queue byte counter may be offset by +/-2 bytes. For any packets originating from the CPU, the per-queue byte counter may be offset by -12 bytes. (97660)
- Packets that attempt to do a GRE key lookup where the GRE key lookup misses will have egress IPv6 ACLs applied with the ingress VLAN (102455)
- GRE key forwarding packets that are recirculated will have no QoS policy applied to them. (102458)

- If a double tagged frame is received on an untrusted or DSCP-trusted interface, the CoS is retained if the outgoing frame is tagged, unless the frame is routed (131614)
- IPv6 Egress ACL deny logging is not supported on subinterfaces. (146487)
- PBR policy is supported only on interfaces in the default VRF. If a PBR policy is configured on an interface in a user defined VRF, the behavior is undefined. (148895)
- Disabling IPv4 routing on an L3 interface is not supported when IPv6 routing is enabled on that L3 interface. When "no ip routing ipv6 interfaces" is configured to enable the forwarding of IPv4 packets over IPv6 nexthops over interfaces that do not have IPv4 address, but only a IPv6 address, it will also allow routing IPv4 traffic over these interfaces. (151356)
- While in Tap aggregation mode enabling either VN or BR tag stripping will disable VXLAN header stripping functionality. Traffic steering on the inner IP header of VXLAN packets will also be disabled.

  Removing the VN/BR tag stripping configuration will restore VXLAN stripping and traffic steering functionality. (175829)
- When the 'vxlan-routing' hardware TCAM profile is configured, VXLAN traffic flows in overlay may not work alongside IPv6 traffic flows in underlay. The workaround is to use the CLI command 'no platform sand ipv6 host-route exact-match'. (190017)
- In Tap Aggregation mode, Tap Aggregation features may not work for 802.1BR/VN tagged packets when 802.1BR/VN tag stripping is not configured. (198798)
- Links are not compatible with systems running EOS 4.18.1F

  The workaround is to upgrade both sides of the link. (199152)
  SKUs Affected: 7500R-8CFPX-LC
- Traceroute to a IP route where the IP route is getting forwarded through a MPLS nexthop-group may incorrectly display the first hop as being unreachable. The actual first hop will appear in the second position. (209273)
- When ingress packet truncation is enabled in Tap Aggregation mode, truncated packets are not counted as packets received on the ingress interface. (215346)
- Frames less than 64 bytes are dropped (as expected),
  but not counted.

  Command "hardware phy cmx42550 <intf > diag read64 mac line 0x138"

can be used to dump the counter for the purpose of debugging". (218429)
SKUs Affected: 7500R2M-36CQ-LC, 7800R3-48CQM-LC, DCS-7280CR2M-30-F, DCS-7280SRAM-48C6, DCS-7280SRAM-48C6-F, DCS-7280SRAM-48C6-R, DCS-7280SRM-40CX2-F and DCS-7280SRM-40CX2-R

- Vxlan decapped packets will not match rules that match on 'tcp established' in egress acls (226582)
- Native VLAN setting on Tap interfaces does not take effect. (227770)
- While in Tap Aggregation mode, ingress VLAN membership filtering does not work when packets are destined to a tool interface configured with egress packet truncation. (227841)
- While in Tap Aggregation mode, interfaces configured for egress truncation will continue to consume hardware resources even when they are down. (228384)
- LLDP functionality is not supported on interfaces with ingress truncation enabled. (229983)
- Sflow agent CPU utilization is around 10% even when hardware acceleration is enabled and the agent is not processing any flow samples. (251674)
- With MTU increased beyond 9100B, there can be some multicast packets of size greater than 9100B that are dropped as a port gets close to linerate. (261446)
- Changing PMF profile on one linecard may cause a brief disruption of PMF-based features on other linecards which should not be affected by the same change. (270849)
- A QoS policy, with a class map which has either set-tc or set-dscp on the ingress port and which has DSCP rewrite map on the egress port, results in indeterministic behavior with respect to DSCP remarking of the outgoing packet. (273320)
- If a QOS and PDP Policy both having police action are applied on an interface and the traffic hits both the policies then QOS Policer Counter is messed up. The "show policy-map type qos pmap-name" will give the PDP Policer Counter, not the QOS Policer Counter. (275994)
- Rate values for subinterfaces shown by "show interface counter rates" may deviate up to 15% from corresponding rate on parent interface. (278700)
- With TCP MSS Clamping feature configured, TCP SYN packets might get dropped under high CPU usage conditions if the incoming TCP SYN packet rate is high. (279370)
- Packets larger than 10196 bytes will be discarded by the forwarding ASICs. (280459)

- PFC on DSCP trusted ports is not supported. (281214)
- Loop protect feature is not supported when AlgoMatch HW is enabled. (290706)
- When a port becomes a LAG member, there may be a very brief moment where a few packets may be duplicated on the LAG. (295260)
- Fragmented IP packets will not match on flow-spec rules that include a match on TCP/UDP port. (297309)
- When all the L2 subinterfaces belonging to a parent interface are shutdown, packets are bridged and mac addresses are learnt on parent interface (300202)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- VXLAN routing is not supported on a modular system on which one of the linecards is configured for TAP aggregation. (306180)
- Show interfaces counters ip only show IPv4/Ipv6/MPLS counters per physical interface and not per port-channel (306209)
- When a BGP peer session is cleared, traffic which hits existing flow-spec rules may increment the wrong counter for a brief period of time. (339523)
- If non shaped sub interfaces are configured under same interface having shaped sub interfaces, traffic will egress out of the non shaped sub interfaces in a round robin fashion. It is recommended to not have shaped and unshaped sub interfaces under the same parent. (341851)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- Hardware accelerated sflow with profile sflowaccel-v2 doesn't work with 7500E linecards. (342130)
- Stale telemetry flow-spec statistics may be seen until the next "show flow-spec" command is issued. (345195)
- Hardware accelerated Sflow does not support collectors reachable over arbitrary tunnel types (354749)
- IPv4 packets with options in the IP header will not be subjected to Unicast Reverse Path Forwarding (uRPF) checks,
  and hence will not be dropped even if the source IP is unknown. (355542)
- unicast RPF is not enforced on IP packets when the destination IP needs ARP resolution (356347)
- Software forwarding is not supported for GRE or IP-in-IP tunnel terminated packets using decap-groups. (358369)
- The egress DSCP value in the Outer IP header for packets that undergo headend

replication after routing is derived from the Traffic Class (and not copied from the ingress DSCP value). (366189)

- While in Tap Aggregation mode, if the identity tag configuration of a Tap port is changed, traffic received on this port may be sent to an invalid multicast destination momentarily. This will cause the DchUnreachables counter to increment. (372757)
- TX mirroring shows VXLAN encapsulated packets that are actually dropped by split horizon. (375795)
- If more than maximum supported Ipsec tunnels are configured, it is random as to which ones are assigned flow entries within on-chip encrypt/decrypt engine. The set of Ipsec tunnel interfaces assigned flow entries may not be the same as the set of tunnel interfaces which have IKE connections established. As a result, some tunnel interfaces with IKE connection established may not get link up. (376431)
- Configuring more than 250 BFD sessions on a physical interface may result in many of those sessions flapping because of hardware drops on the interface. (389387)
- Drop Precedence based tail drop thresholds can be ignored when multiple queues are congested and buffering resources are low. (395693)
- If a security-ACL is configured on a sub-interface beyond the supported limit of acls,
  SandAcl might restart continuously until the number of configured acls is brought back within the supported limits (398815)
- Queue build-up doesn't show up for 64 byte packets in case of congestion via following commands:-
  1) platform fap diag diag cosq non_empty_queues
  2) show interfaces queue length

  Following command should be used instead:-
  show queue-monitor length (398937)
- PIM sparse mode feature which allows installation of outgoing interfaces on the non-DR for a faster failover does not work on L3 sub-interfaces. This feature relies on an egress ACL to stop multicast traffic from going out of the interface. Multicast egress ACLs do not work on L3 sub-interfaces due to a platform limitation. If the feature is configured, there will be duplication of traffic. The workaround is not use the feature on such interfaces. (405696)
- When a policy-map with match on inner VLAN is programmed on an interface, if single tagged packet traffic is sent to that interface, the behaviour of that packet is indeterministic as inner VLAN tag is calculated using an

offset and vlan-tag-format qualifier doesn't differentiate between single and double tagged packets. (415587)

- When MPLS label is pushed on the traffic ingressing CoS trust port then EXP bits are not derived from TC based on packet's COS. (417108)
- Byte counts are not supported for IPSec tunnels. (419031)
- SflowAccel supports up to 200 VRFs. (423892)
- PAUSE frames with correct DMAC=01:80:C2:00:00:01, Ethertype=0x8808, opcode=0x0001 are never forwarded and are always consumed by the hardware. (426047)
- Header truncation for mirrored packets can not be used when the destination of a monitor session is a GRE tunnel. (428547)
- A port transmitting packets smaller than 100B that were tunnel terminated on the switch might be limited to ~90% linerate (429797)
- Egress MAC ACLs are matched on the incoming packet's ethernet header and not on the rewritten ethernet headers. (458724)
- IPv4/IPv6 counters are not supported on port-channel interfaces. (479658)
- Egress mac acls do not work on interfaces that are not front-panel interfaces, even though they can be configured. (483583)
- When the feature "flow" in a TCAM profile is configured with only the "drop" action, the profile is rejected. The workaround is to add any other action to feature "flow". (486849)
- When a LAG is used as a destination for a monitor session, a given set of packets mirrored from a Rx source will hash differently compared to the same set of packets captured from a Tx source, due to hardware limitations. Consequently, symmetric hashing will not work as expected with a monitor session which captures both Rx and Tx traffic from a single port, and using a LAG as a destination.

  A workaround is to only capture traffic on the ingress (Rx direction). Another workaround is to use two different monitor sessions, and destinations, for the two directions of the target traffic, and implement symmetric hashing on a second stage. (486994)
  Series Affected: DCS-7020, DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series

- Lag subinterfaces are not currently supported in pseudowire or local-local patches (i.e. a patch with two local interfaces). (490834)
- Egress MPLS tunnel counters are not supported for implicit null tunnels. (496375)

- When "ip hardware fib optimize" is enabled for a non-nibble aligned prefix-length, local-remote MPLS Pseudowires must have Control Word enabled for MPLS decap forwarding to work correctly. If Control Word is not enabled, then ETHoMPLSoETH traffic that ingress with the first nibble of the inner DMAC starting with "0x4" will be speculative parsed as IPv4oMPLSoETH and incorrectly dropped. (496624)
  Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- While a switch is in Tap Aggregation mode, if the total number of FAPs on all linecards in Tap Aggregation mode is more than 73, then some Tap Agg features, e.g. MPLS Pop, may stop working on some FAPs, due to insufficient hardware resources. When this happens, the message "Hardware resources are insufficient to program all entries in ISEM-A table" will be logged. (498192)

- For Packets with GRE tunnel encap header, MTU enforced on the hardware is 3 bytes more than configured value in Cli. (498470)
  Series Affected: DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- With 'hardware next-hop fast-failover' configuration, the maximum ECMP size supported is reduced to 1023 in R, R2 series and 127 in R3 series swtiches respectively. (502940)

- VRF label termination into non-default VRF is not supported for multi-label MPLS packets. (504763)

- When BGP neighbors advertise Flowspec rules with police actions where the number of rules exceed what can be programmed in TCAM, policers will be allocated in hardware for all requested rules even though best-effort programming will only program the subset of rules that fit in TCAM. As a result, hardware policer resources will be unnecessarily consumed for rules which are not installed in hardware. (506688)

- Egress counter features configured via "hardware counter feature ..." do not include packet or byte counts for packets sent from the local CPU. (525380)

- With flex-route compress option enabled or the flex-route internet profile along with a hardware tcam profile including the flex-route feature, if the default route resolved over tunnel, it may lead to SandL3Unicast agent to restart continuously. (525611)

- Counter information flows from the forwarding chips to the tables that support TerminAttr in a very bursty manner. When averaged over a several minute window the rates will be accurate, but for shorter intervals calculated rates may oscillate significantly above and below the nominal rate.

For better accuracy, please use a longer interval to generate rate information. (540116)

- Hitless restart is not supported with Macsec proxy (540419)
- `show forwarding destination` may give incorrect results when the traffic would hit an egress IPv4 ACL using bridged IPv4 traffic or hit an egress IPv4 ACL using one of the following qualifiers: TCP established, fragment, and L4 port range. Note that TCP and UDP egress IPv4 ACL rules use the fragment qualifier. (554480)
  Series Affected: DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series
- Hitless restart of Layer 3 forwarding agent is not supported unless "ip load-sharing prefer local" configuration is removed. Note that this configuration is added by default on this system. (555772)
  SKUs Affected: DCS-7280QR-C36
- "shape rate" configuration is not supported on LAG subinterfaces used for MPLS pseudowires. (555799)
- Route churn under hardware FIB exhaustion may cause BFD sessions to flap. (556089)
- MPLS label popped packets will not match rules that match on 'tcp established' in egress IP acls (565015)
- For products with paired QSFP100 (odd numbered) and QSFP+ (even numbered) ports, the even numbered port may experience link flaps when a transceiver with a different media type from the previous installed transceiver is inserted in the odd numbered port. (565969)
  SKUs Affected: DCS-7280QR-C72-F, DCS-7280QR-C72-M-F, DCS-7280QR-C72-M-R, DCS-7280QR-C72-R, DCS-7280QRA-C36S-F and DCS-7280QRA-C36S-R
- VRRP IPv6 using VRRP IPv4 MAC prefix may have unexpected packet forwarding behavior when the VRRP IPv6 and IPv4 have different states and one of the states is Master. (567504)
- Routes resolved over LAG sub-interfaces that have shape rate configured may forward traffic to CPU after SandL3Unicast agent restarts. The workaround is to flap the parent LAG by using the shut and no shut command. (570311)
- PE to PE overlay ping does not work on L2 MPLS EVPN. Work around isn't available. (617720)

DCS-7280R and DCS-7500R Series

- An IPv6oMPLS packet terminated by L3 EVPN MPLS configuration will not be forwarded. The workaround is to disable IPv6 exact match host routes using 'no platform sand ipv6 host-route exact-match' and disable IPv6 route

optimizations for prefix length 128. (201414)
Series Affected: DCS-7020, DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series

- When a linecard is inserted in a chassis there can be a temporary marginal drop in fabric throughput for other cards. (205880)
- On the system with DCS-7500R linecards, if DCS-7500R2 linecards are inserted, routes may consume more resources in the hardware routing table. (215393)
- Jericho chip buffering DRAM test at agent startup does not catch bad parts while it should fail to force RMA of bad parts. (218971)
- VXLAN and GRE tunnels cannot be configured at the same time. (248239)
- IPv6 multicast routes are stored in two separate TCAM resources. The group IP is stored in one TCAM while the source IP is stored in another. Since one TCAM contains the source IP it will contain an entry for every multicast route. However, the group IP TCAM will reuse entries for duplicate group IPs. For example, if you have routes (S1,G1) and(S2,G1), one TCAM entry is required for the group IP and two TCAM entries are required for the source IP. This means it is possible that more TCAM resources are allocated to the source IP lookup than the group IP lookup. The scaling achieved during the initial distribution of multicast routes will be preserved. However, if the distribution later changes, optimal scaling for the new distribution may not be reached. (257364)
- The CPU traffic policy feature does not support filtering on IPv6 extension headers. (364996)
- Ingress ACLs and PBR are not supported for MPLS tunnel terminated traffic using VRF label. (366695)
- VRF terminated traffic is not sampled with sFlow. (369010)
- Drop-precedence thresholds are not supported on mirror session ports. (388932)
- We do not support incoming multicast LDP packets with a destination multicast MAC address.
  RFC 5332 doesn't mandate the use of sending labeled multicast traffic in a multicast ethernet frame. Multicast MAC destination address could be used in upstream label assignment. (393406)
  Series Affected: DCS-7020, DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series
- Egress Ipv4 ACLs and Egress MAC ACLs cannot be configured together (443671)
- Egress Ipv6 ACLs and Egress MAC ACLs cannot be configured together. (443673)

- With `counters per-entry` for egress mac acl, we can uniquely count max of 3967 rules per fap. (460819)
- MTU is not enforced for MPLS packets forwarded by a MPLS swap route, which have a length one byte more than MTU. (464742)
- The two rate three color (trTCM) QoS policy-map counters can show incorrect values for packets marked green or yellow if the ingress traffic is broadcast or multicast traffic. (479267)
  Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7500R and DCS-7500R2 Series
- L2VPN or VPWS resolution through SR-TE tunnels consisting of 5 or 6 label stack isn't supported. (494953)
- If the CPU is included in monitor sessions with multiple destinations, it will only work if the device mirror0 is selected. If multiple mirroring to CPU sessions with multiple destinations are configured, all packets will be sent to mirror0. (525919)
- SandAcl agent may restart a few times when other Sand agents restart. (546778)
- With RFC5549 ACLs configurations, the Egress IPv6 ACL deny logging on port channel subinterfaces stops working on performing agent SandL3Unicast restart. (549181)
- MPLS explicit NULL termination isn't supported with flex-route configuration containing non-nibble aligned prefix length. (576801)

DCS-7280R2 and DCS-7500R2 Series

- On platforms with Jericho+ switches and with large number of pseudowire patches (2500 or more) configured, disabling hierarchical FECs (HFECs) using CLI command "ip hardware fib hierarchical next-hop disabled" may leave some patches unprogrammed and not operational.

  Workaround is to save config with HFEC disabled to startup config and reload the switch. (569868)

DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series

- "Drop" MAC entries only drop packets whose destination MAC address matches the "drop" MAC entry. Packets whose source MAC address matches the "drop" MAC entry are not dropped by the "drop" MAC entry. (341123)
- With "match mpls" PBR configuration, MPLS packets matched both by PBR and a LFIB route with a pop action would get forwarded correctly only if the MPLS route contains "access-list bypass" configuration. (370118)

- Strict Priority scheduling for 400G interfaces don't work properly for 64 byte packets when traffic rate is above PPS limit of the chip. (388517)
- Cli to change tail-drop threshold for 200/400G ports is not supported by software. (396029)
- IP forwarded traffic that is mirrored to a GRE tunnel destination will have the PCP bits of their VLAN tag set to 0. (400909)
- Traffic drop may happen when we sent traffic to all 8 traffic-classses (aggegrate rate nearing linerate) to port which has been configued with Strict-Priority scheduling. (406550)
- Traffic drop may happen when we sent traffic to all 8 traffic-classes (aggregate rate nearing linerate) to port which has been configured with WRR scheduling. (406561)
- Only port-channel interfaces are supported as peer links. Single member port-channel interfaces are supported. (409958)
- Per TC based VOQ tail-drop thresholds isn't supported in software. (413344)
- Application of low rate shaping on multiple interfaces with line-rate traffic into the box will create a backlog in DRAM. Due to this majority of traffic will be served to egress from slower DRAM instead of SRAM. In the congestion state , even after the removal of shaping with line-rate traffic ingress from multiple ports, switch won't be able to deliver full throughput. The recovery from DRAM to SRAM will happen over a period of time once the congestion is removed. (414481)
- Set dcsp will not apply to mpls routed packets that egress with mpls labels (418791)
- Unidirectional links are not supported at 40G speed on QSFP100 interfaces using the CRT50216 PHY. (467672)
  SKUs Affected: 7368-16C, 7500R3-36CQ-LC, 7500R3K-36CQ-LC, 7800R3-48CQ-LC, 7800R3-48CQM-LC, DCS-7280CR3-32D4, DCS-7280CR3-32D4-F, DCS-7280CR3-32D4-M-F, DCS-7280CR3-32D4-M-R, DCS-7280CR3-32D4-R, DCS-7280CR3-32P4, DCS-7280CR3-32P4-F, DCS-7280CR3-32P4-M-F, DCS-7280CR3-32P4-M-R, DCS-7280CR3-32P4-R, DCS-7280CR3-96, DCS-7280CR3-96-F, DCS-7280CR3K-32D4, DCS-7280CR3K-32D4-F, DCS-7280CR3K-32D4-R, DCS-7280CR3K-32P4, DCS-7280CR3K-32P4-F, DCS-7280CR3K-32P4-R, DCS-7280CR3K-96 and DCS-7280CR3K-96-F
- Certain speed groups are limited to one active serdes rate configuration. These speed groups are those that show only one serdes rate in the Active column of the output of "show hardware speed-group status". (486659)
- For VXLAN decapsulation + routing of overlay packet, the ECN bits may not be correctly copied from the incoming overlay packet. (489998)

- VXLAN VARP VTEP with IPv6 overlay routing requires vxlan-routing TCAM profile to be applied on the switch. (503496)
- The "phy link serdes mapping direct" CLI command requires the 25g serdes rate to be configured, unlike what is displayed in "show hardware speed-group configuration". (523850)
  SKUs Affected: 7500R3-36CQ-LC, 7500R3K-36CQ-LC, 7800R3-48CQ-LC, 7800R3K-48CQ-LC, DCS-7280CR3-32D4, DCS-7280CR3-32P4, DCS-7280CR3-96, DCS-7280CR3K-32D4, DCS-7280CR3K-32P4, DCS-7280CR3K-96, DCS-7280CR3MK-32D4 and DCS-7280CR3MK-32P4
- Encapsulating PTP packets over VXLAN tunnel is not supported. (526461)
- When SandCounter agent is down, datagram counters are not accounted. Hence in show sflow output, the "Number of Datagrams" entry displays lesser value than expected. (536213)
- If all front-panel ports are populated, and traffic load is high, an improperly programmed current limit could be exceeded generating a spurious power-off. (536331)
  SKUs Affected: DCS-7280CR3-96 and DCS-7280CR3K-96
- Symmetric hashing is always on for IPv6 addresses, when both source and destination addresses are included in the applied load-balance profile. (557714)
- ECN bits are not preserved during VXLAN bridge encapsulation (587486)

DCS-7020 Series

- The interface bin counter for both in and out packets with sizes 1523-Max may be inaccurate. Packets with sizes between 9217-9236 are not counted by the switch for interfaces Ethernet 1-48. (188121)
- Mirroring and sFlow can not be supported on the same source interface at the same time due to a hardware limitation. (209060)
- AES128/SHA-1 and AES256/SHA-256 are the only supported encryption/ authentication algorithm pairs. (342005)
  SKUs Affected: DCS-7020SRG-24C2-F and DCS-7020SRG-24C2-R
- Using an Ipsec tunnel interface for policy-based routing nexthop is not supported. (378861)
  SKUs Affected: DCS-7020SRG-24C2-F and DCS-7020SRG-24C2-R
- Ipsec tunnel interfaces are not supported as part of nexthop-group. (378890)
  SKUs Affected: DCS-7020SRG-24C2-F and DCS-7020SRG-24C2-R
- Dynamic NAT, AKA Port Address Translation, is not supported for IPSec tunnels. (384624)

DCS-7020R, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- If a packet is mirrored to a GRE tunnel, but the forward copy is trapped to the CPU, then the ingress VLAN ID carried in the GRE key will be set to 0 when the mirrored copy is encapsulated in the GRE envelop. (434871)
- Mirroring to GRE destinations will not work if VxLAN encapsulation is enabled (548429)
- Different streams being rate-limited by the same group policer might exhibit bias towards some streams and fair policing across all the streams is not guaranteed. (578041)
  Series Affected: DCS-7280CR2, DCS-7280R, DCS-7280R2, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500R and DCS-7500R2 Series
- L4 destination port matching in egress IP ACLs does not work on untagged bridged traffic. (609461)

DCS-7280R3, DCS-7500R3 and DCS-7800R3 Series

- If a packet that is decapsulated with a decap group is mirrored to a GRE tunnel, the packet's ingress VLAN will be set to 0 in the upper 2 bytes of the GRE key. (430986)
- QoS policy-map is not supported on Pseudowire decapsulated traffic flows. (574600)
- Renamed TCAM Qualifiers l4ops_ip_pacl, l4ops_ip_qos, l4ops_ip6_pacl, and l4ops_ip_racl into l4ops_24b, l4ops_7b, l4ops_3b and l4ops_18b. This can cause customer scripts using `show platform fap pmf` command to fail if they are using any of the above renamed TCAM qualifiers. (595868)
- On Gen4 Faps , SSO is hit full for TCAM based ACL rules. (606764)

DCS-7280R and DCS-7280R2 Series

- Flex-route is not supported with security ACLs (Port ACLs, Router ACLs & MAC ACLs) when AlgoMatch is enabled. The workaround is to configure 'hardware access-list mechanism tcam'. (348149)
- CBF does not work in AlgoMatch mode on some custom TCAM profiles (603206)

7300X3, 7320X, 7368, CCS-720XP, DCS-7010, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7060X4, DCS-7250X, DCS-7260X, DCS-7260X3 and DCS-7300X Series

- Untagged packets received on a port with PFC enabled may be assigned the wrong priority. In case of congestion, PFC frames may not be sent or may be

malformed.

The issue is observed when a port uses a default CoS value that is mapped to a traffic class with a different value. For example, if the default CoS is 0 and CoS 0 is mapped to traffic class 1. The workaround is to change the default CoS value on the port or the global QoS mapping such that the default CoS and the traffic class match. (23922)

- System does not stop transmitting traffic for the exact amount of time quanta received in PAUSE or PFC frame. This can lead to packet loss during congestion if the peer switch does not have enough buffers. The workaround is to use XON/XOFF instead of time based flow control, or to increase the time to account for one MTU sized packet. (27190)
- QoS shaping and guaranteed bandwidth will only work in store-and-forward mode. They are not supported in cut-through mode. This includes 'shape rate X' and the 'bandwidth guaranteed X' commands. (56790)
- Accelerated Software Upgrade (ASU) from 4.13.x (x < 6) to 4.13.6 and above requires a special upgrade procedure due to a software image format change. (90097)
- 10 Gbps packet replication on all SFP+ ports at the same time may lead to packet discard. (91149)
- Egress L2 MTU violations in cut-through mode may result in unexpected discards of other frames. (95577)
- VXLAN encapsulated packets cannot be TX mirrored at the egress properly. The mirrored packets will have an incorrect MAC header. (97272)
- Forwarding-table partition mode 4 is not supported. (100862)
  Series Affected: DCS-7010 Series
- When IGMP snooping is enabled a single unknown multicast floodset is shared across all VLANs with IGMP snooping enabled. This can cause unexpected flooding to a trunk port that has no multicast routers on a given VLAN, but has multicast router attached to the same trunk port on another VLAN. (105188)
- When "hardware access-list resource sharing vlan in" is configured, systems will start sharing resources that are required for programming access-group/ access-list. In this mode only 24 port range checkers are available for programming L4 port ranges. After the 24 port range checkers are consumed, system will use port number and mask combination to program the rules in the access-list. Doing so would result in a given access-list consuming more TCAM entries in this mode than it would in the default mode. However, as the access-list is shared among multiple VLAN interfaces the effective TCAM usage can be lower.

This affects ip access-list, ip standard access-list, and ipv6 access-list. ipv6 standard access-list
is not impacted. (105498)
Series Affected: DCS-7010, DCS-7050X and DCS-7050X2 Series

- "hardware access-list resource sharing vlan in" configuration will not share resources required by IPv6 standard access-lists. (105502)
  Series Affected: DCS-7010 and DCS-7050X Series

- When "hardware access-list resource sharing vlan in" is configured, Link Local Multicast traffic will not be intercepted by the ACL attached to the VLAN interface. (105504)

- A large ACL and PBR policy configuration that consumes all TCAM resources may not fit after doing a config-replace, ACL agent restart or switch reload. After performing a config-replace, ACL agent restart or a switch reload, it is possible that only the ACL or the PBR policy will be able to fit. (105667)
  Series Affected: DCS-7010 and DCS-7050X Series

- There may be a momentary traffic disruption every time the nexthop specified in a PBR policy resolves to a new destination: affected packets may be forwarded by normal L3 lookup, or be dropped.

  The system will recover automatically; the PBR policy will return to route packets as per the new nexthop resolution momentarily. (105670)

- When any PBR policy is applied, packets that violate the egress MTU and are destined to flood the VLAN will end up being flooded instead of being sent to the CPU. (105680)

- Subinterfaces cannot be used to send or receive VXLAN encapsulated packets. (105767)

- When "hardware access-list resource sharing vlan in" is configured, changing the ACL on a VLAN interface:

  1. From an ACL that is not shared with other VLAN interfaces to one that is shared with other VLAN interfaces can cause deny traffic to get permitted until the new ACL takes effect.

  2. To another ACL that doesn't fit in the TCAM can cause deny traffic to get permitted until the system reverts back to the previously applied ACL. (106646)

- If IP-in-IP decap groups are configured, "qos trust dscp" configuration is not supported on traffic matching the decap groups. (107579)

- Vxlan and MPLS features may not be configured at the same time. (109330)

- When "hardware access-list resource sharing vlan in"" is configured and TCAM is close to being full, restart of the forwarding agent or a reboot of the box, can cause some ACLs to not get programmed properly. (109876)
- The Accelerated Server Upgrade feature is not supported with the "hardware access-list resource sharing vlan in" configuration. (110114)
- IGMP snooping is not supported on Vxlan enabled VLANs. The multicast packets will always be flooded locally and to remote VTEPs. (110479)
- A front-panel or fabric port may get stuck in an errored state and drop traffic egressing the port. When this happens, the forwarding agent log will contain "port <internal port #> start error detected". This condition will persist until it is manually cleared. A forwarding agent restart is required to clear the error and forward traffic normally. (112051)
- MPLS is not supported on subinterfaces. (113110)
- Packets being VXLAN encapsulated are constrained to a single underlay physical nexthop per physical egress port.

  Topologies involving SVIs over trunk ports, or non point-to-point routed ports towards the core will not work optimally, the encapsulated packets will be sent to the wrong next-hop for all but one of the VTEPs.

  Topologies involving virtual VTEPs connected via a downstream L2 switch will not work, as the receiving vswitch will not have the capability to route the packet to the right VTEP. (113722)
- Port ACLs are not supported on VXLAN terminated traffic. (113726)
- If the configured RACLs do not fit in the TCAM, then disabling the RACL sharing feature might cause removing a RACL from an individual VLAN interface to fail.

  To recover from this state, delete/remove the access-list and then reconfigure the access-list. (114028)
- Configuring "hardware access-list resource sharing vlan in" in a config replace session or in config session is not supported (114291)
  Series Affected: DCS-7010 and DCS-7050X Series
- L2 flooding of BUM packets on Vxlan vlans uses L3 replication tables, which are also used by IP multicast routing. The replication tables have an entry for each vlan, physical port combination (lag or non lag). We will run out of this table resources if we need more than 64k entries. (114517)
- Toggling "hardware access-list resource sharing vlan in" configuration could cause ACLs that were already programmed on VLAN interfaces to not get programmed. This could traffic loss on the VLANs where the ACLs were

originally applied. (115348)
  Series Affected: DCS-7010 and DCS-7050X Series

- If the switch is in cut-through mode, L2 MTU violations will not be counted if the packet headers are changed while forwarding. (116760)
- QoS policies are not supported for L3 Unicast flooded packets (routed packets with nexthop MAC not learned) (123883)
- When a PBR is attached to any interface, Layer-3 packets which are getting flooded in the egress VLAN will not be treated with Egress Router ACL if one is configured on that egress VLAN. (133144)
- VXLAN routing is not supported on systems with
  BCM56750 fabric chips. Such switches can be identified using the CLI command "show
  platform trident l3 summary", which will show bcm56750 for "Fabric chip model". (134625)
- Mirroring of incoming multicast traffic to a GRE tunnel may result in data traffic loss on the egress interface in an oversubscription scenario. (139591)
- Egress IP/IPv6 router ACL is not supported for VXLAN encapsulated traffic. (148642)
  Series Affected: DCS-7050X2, DCS-7050X3 and DCS-7300X Series
- IP ACLs configured on SVIs to match routed IP multicast traffic may also match bridged IP multicast traffic in that SVI. (152523)
- If hardware tables for VLAN translation overflows, the entries need to be un-configured and re-configured after the overflow condition is removed due to appropriate configuration changes. (157196)
- Up to 4 mirroring sessions are supported.

  Each direction mirrored on a source port counts towards that limit of 4. For example, if a port is configured with rx and tx mirroring (the default), this counts as 2 consumed sessions. (158490)
- 1) Multicast traffic matching reserved IPv4 multicast address range 224.0.0.X is not counted by L3 interface counters.
  2) L3 interface counters not supported for IPv6 multicast traffic.
  3) Unicast traffic to CPU is counted by L3 interface counters only if routing is enabled (i.e. ip routing for IPv4 traffic and ipv6 unicast-routing for IPv6 traffic) (160930)
- Mirroring of Vxlan encapsulated packets in the egress direction is not supported. (167189)

- If a trunk port is configured as a member of both the underlay and overlay VLANs, the following limitations apply:
  - If packets received on the trunk port are flooded in the overlay VLAN, the VxLAN encapsulated copy is not forwarded on the ingress trunk port.
  - Vxlan encapsulated packets received on the trunk port, if flooded in the overlay VLAN after decapsulation, are not forwarded on the ingress trunk port. (185321)
    Series Affected: DCS-7050CX3, DCS-7050SX3, DCS-7050X2 and DCS-7300X Series

- If ingress ACL is applied on an interface, traffic sent to CPU from that interface is falsely counted as InAclDrop in "show int counters ingress acl drop". (203465)

- Clause 37 auto-negotiation on SFP28 and QSFP28 ports is not supported. A workaround is to use 1G forced speed configuration on the affected ports. (206778)
  Series Affected: 7300X3, CCS-720XP, DCS-7050CX3, DCS-7050SX3, DCS-7050TX3, DCS-7050X3, DCS-7060CX, DCS-7060CX2, DCS-7060SX2, DCS-7060X, DCS-7060X2 and DCS-7260CX3 Series

- When "reload fast-boot" is performed from a release prior to 4.17.2, switches with BGP peering connections with the switch undergoing "reload fast-boot" could experience BGP KeepAlive timeouts before they see port flaps. This could result in longer than expected data plane downtime during the upgrade. (214700)
  Series Affected: DCS-7050X, DCS-7060X and DCS-7060X2 Series

- A multi-bit ECC error in forwarding ASIC packet memory cannot be automatically corrected. A hitful restart of the slice agent managing the forwarding ASIC or a reboot of the system is required to clear the condition. (214950)

- If ip-ttl is the only enabled field for port channel hashing, after reload hitless, packets may get hashed to a different link than before the reload. (223568)
  Series Affected: DCS-7050TX, DCS-7050X and DCS-7060X Series

- A configured mirroring ACL may not be applied in hardware. This can be confirmed by checking the output of 'show platform trident tcam mirror'. (236908)

- When a VXLAN encapsulated packet is received on a VXLAN VLAN where PBR policy is applied, the switch will not PBR forward the decapsulated packet. (244093)

- Sflow output interface determination will not work when the output interface is a subinterface. (250424)

- A switch may not be able to bridge or route VXLAN traffic if it hits one or all of following conditions:
  - Nexthop resources are exhausted as indicated by syslog VXLAN_HWHER_NEXTHOP_RESOURCE_FULL.
  - MAC table overflow as indicated by show platform trident mac-address-table missing.

  To recover from this condition reduce the config scale and flap the VXLAN interface. (253601)
- Flexible port-channel hashing may not hash accurately when the inner L4 header option is configured for IPV6 GRE packets. (267487)
- If a packet stream is policed by multiple policers, the policed rate may be lower than any of the configured policer rates. (271046)
- To perform filtered mirroring of a packet based on VLAN from an interface configured to perform VLAN translation, the ACL must be programmed with the translated VLAN. The mirrored packet will be the same as the packet at the source interface. (278599)
- BGP neighbor sessions may flap when URPF is configured on an interface. (279113)
- To perform filtered mirroring of a packet based on VLAN from a subinterface source, the ACL must be programmed with the internal vlan of the subinterface. The mirrored packet will be the same as the packet at the source interface. (280943)
- Matching on inner VLANs is not supported in mirror ACLs. If an entry is specified matching on inner VLAN, it will be ignored and permit all packets. (284371)
- SSU is supported when upgrading from the associated release in each release train: 4.18.8, 4.19.8, 4.20.7, 4.21.0. (289548)
- Issuing "no shutdown" on a member link of port-channel may send duplicate packets for sub-second on that member link (291514)
- DirectFlow (and features such as the MacroSegmentation Service that use DirectFlow) are unsupported on the 7260, 7300 series of switches. (296715)
- When primary vlan and secondary vlan are part of different MST instances, the hardware programming of lag will not happen. (300119)
- Not all interfaces in the groups Ethernet49-Ethernet52 and Ethernet53-Ethernet56 can be broken out in to 4x25G, 4x10G or 2x50G mode due to MAC resource limitation on the system. Interfaces without MAC resource will be marked inactive and 'STRATA-4-HW_PORT_RESOURCE_FULL' will be logged in syslog.

Speed change on interfaces in the groups Ethernet49-Ethernet52 and Ethernet53-Ethernet56, can free up the MAC resources to make inactive interfaces active in that group. (306121)
SKUs Affected: DCS-7050SX3-48YC8-F, DCS-7050SX3-48YC8-R, DCS-7050TX3-48C8-F and DCS-7050TX3-48C8-R

- When MLAG peer MAC routing is enabled, OSPF neighborship over VXLAN overlay may never get established. (349242)
- Ip-length based rules are not supported on Egress ACLs. (353247)
- Packets dropped in the egress pipeline may still be egress mirrored successfully. (357609)
- Some ports (esp. Et73-Et96 and Et103-Et104) might blackhole traffic or fail to linkup. (358362)
  SKUs Affected: DCS-7050TX2-128-F and DCS-7050TX2-128-R
- SSU is not supported with Vxlan and MLAG config. (388669)
- Ports with ingress MAC ACL still learn MAC addresses although traffic may be dropped (400211)
- Reload hitless from EOS-4.22 or earlier results in /2 and /4 ports on Ethernet 1-12, 21-44 and 53-64 to remain inactive when /1 and /3 are configured in 10G or 25G. In order to activate /2 and /4 ports, configure 40G, 50G or 100G /1, then configure 10G or 25G back. These ports are also activated following a forwarding agent restart. (409057)
  Series Affected: DCS-7260CX3 Series
- "reload fast-boot" is not supported with virtual IP address config. (411323)
- Speed change on a port with macsec enabled is not supported and could cause the port to get into a persistently un-authenticated state. Workaround is to disable macsec on the port, change the speed and then re-enable macsec on the port. (415737)
  SKUs Affected: DCS-7050CX3M-32S-F and DCS-7050CX3M-32S-R
- Performing SSU from any release prior to 4.22.2 can lead to extended outage and mis-forwarding. (424812)
  SKUs Affected: DCS-7050SX3-48YC8-F and DCS-7050SX3-48YC8-R
- IP ACL match over MPLS Encapsulated Packets is not supported. (426413)
- During Mpls PHP operation inner payload type gets ignored. (428546)
- When both "hardware counter feature vni decap" and "hardware counter feature vni encap" are enabled, the egress flexcounter pools will only be released after both features are disabled. (441887)
  Series Affected: 7300X3, 7320X, 7368, CCS-720XP, DCS-7050X, DCS-7050X2,

DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7060X4, DCS-7250X, DCS-7260X, DCS-7260X3 and DCS-7300X Series

- When 'hardware nat static access-list resource sharing' is in the switch's config,
  and a static NAT filter ACL and a security ACL have overlapping rules, the security
  ACL's hit counter might not increment in all cases. Regardless of the hit counter,
  both the security ACL rule and the NAT filter ACL rule will be applied correctly.

  Workaround is to disable static NAT ACL resource sharing with:
  'no hardware nat static access-list resource sharing'
  Alternative workaround is to disable port ACL in VFP with:
  'platform trident tcam port-acl vfp disabled' (450080)

- When an interface undergoes a hitless speed change, sFlow sample numbers and sequence counts for that interface may be reset. (452949)
  Series Affected: 7300X3, 7368, DCS-7050X3, DCS-7060X4 and DCS-7260CX3 Series

- With VXLAN dataplane learning disabled, locally learned MAC addresses will not age out if VXLAN encapsulated packets from remote VTEPs are received with inner packet's source mac as the locally learned MAC. The locally learned MAC entry needs to be cleared manually by issuing 'clear mac address-table dynamic vlan <VLAN> address <ADDRESS>'. (460607)

- If the incoming packet is VLAN tagged, then the truncated mirrored packet will be 4 bytes shorter than expected. (463986)
  Series Affected: 7300X3, 7368, CCS-720XP, DCS-7050X3 and DCS-7060X4 Series

- If virtual mac address of the switch is learnt against a front panel port, it may not age out. The workaround is to clear the mac address manually by issuing 'clear mac address-table dynamic vlan <VLAN> address <ADDRESS>' command. (470965)

- When IPV4 and IPV6 PBR are both programmed in TCAM, forwarding plane agent restart may result in IPV6 PBR rules not being programmed in hardware. (473582)

- By default, configuring a static NAT rule with an empty access-list is treated the same as no access-list: for source NAT, the switch will ignore the destination IP, and vice versa for destination NAT.
  With "hardware nat static access-list resource sharing" enabled, configuring a static NAT rule with an empty access-list is treated the same as an undefined access-list: some hardware resources may be consumed, but the traffic will be forwarded untranslated. (473783)
  Series Affected: CCS-720XP, DCS-7050CX3 and DCS-7050X3 Series

- The total length field in the IP header is not populated correctly when operating in cut-through mode. The switch should be operated in switch-and-forward mode when mirroring to a GRE tunnel. (475273)

- Mirrored packets that violate the MTU requirements will not be fragmented. (481513)

- When persistent port security is enabled on an interface, MAC addresses will persist when an interface is down. While the interface remains down, traffic destined to these MAC addresses will be dropped.

  Persistent port security is enabled by default, and can be disabled with `switchport port-security persistence disabled`. (485828)

- If dynamic load balancing is enabled for an ECMP group, it's member link flap might cause poor traffic distribution. Traffic distribution may improve over time. (487595)
  Series Affected: DCS-7060X4 and DCS-7260X3 Series

- If dynamic load balancing is enabled for ECMP groups while the traffic is flowing, then the load on the ECMP members may not be distributed uniformly. Traffic distribution may improve over time. (490418)
  Series Affected: DCS-7060X4 and DCS-7260X3 Series

- When dynamic load balancing is enabled, If multiple traffic flows destined to the same ECMP group arrive at the same time, then the load on the ECMP members may not be distributed uniformly. Traffic distribution may improve over time. (490716)
  Series Affected: DCS-7060X4 and DCS-7260X3 Series

- Packets sent from the CPU cannot be egress mirrored unless they are being sent out of an SVI. (495146)

- If the speed of an interface changes with traffic running, it is possible for "show interface counters" and "show interface counters fast-poll" to diverge on that interface. (502252)

- Egress mirroring of multicast packets that are going to be encapsulated on the switch, independent of mirroring, is not supported. (512880)

- The mirroring logic can only capture and mirror packets seen by the ingress pipeline. Packets generated by the memory-management unit do not traverse the ingress pipeline and hence cannot be mirrored. This applies to all types of mirroring. (527668)

- When policer is attached to the class-default of an egress policy-map consisting of both IPV4 and IPV6 ACLs, IPV4 and IPV6 traffic hitting class-default would be policed individually with rate configured on default class-map (541843)

- The Strata agent restarts after running "platform trident diag psr <port>" command. (546588)
- Routing between VXLAN VLANs with VRRP is not supported. (548160)
  Series Affected: DCS-7050QX, DCS-7050SX, DCS-7050TX, DCS-7050X, DCS-7060CX, DCS-7060CX2, DCS-7060SX2, DCS-7060X and DCS-7060X2 Series
- The traffic load across ports comprising a port channel(s) may be uneven for certain traffic patterns and/or port channel configuration and state.

  Workaround:
  - change the seed in the hashing algorithm until satisfactory result is achieved by executing configuration CLI command:
    "arista(config)# port-channel load-balance trident <seed>" (555833)
- Implicit ICMPv6 permit rule(s) in TCAM is not seen in output of "show platform trident tcam acl detail" command.

  Workaround is to check the entry and packet hits for the entry using output from "show platform trident tcam detail". This command shows all ACL entries in TCAM and packet hits per entry. (563228)
- Enabling L2 protocol forwarding of LLDP on a given port will implicitly enable forwarding of EAPOL and MKA packets on the same. (569478)
- BGP packets are ignored by IP counters if hardware IP counters are not enabled. (599275)
- Reaching a VLAN's configured limit for locally learned dynamic MACs will not generate a syslog message. (631035)
- The "show tech-support" command does not contain output from the "show mac address-table dynamic local limit" command. (631039)

DCS-7010 Series

- IEEE 1588 PTP transparent clock does not decrement TTL for PTP routed packets (55078)

7320X, DCS-7060X and DCS-7260X Series

- When in cut-through forwarding mode, mirror sessions with both ingress mirror sources and egress mirror sources configured to mirror packets to the same mirror destination port will not be programmed in hardware.

  The workaround for this is to switch to store-and-forward mode where the limitation is not present. (154721)
- Cut-through mode is not supported on the SFP+ interfaces. (182728)

- Cut-through mode is not supported at 1G speed. (219427)

DCS-7260X3 Series

- Configuring 100G, 50G, 40G, 25G and 10G simultaneously might result in unexpected packet forwarding behavior. (235075)

7368 and DCS-7060X4 Series

- Multicast replication resources in TH3 are only 10% of their unicast counterparts. Due to this multicast replication in TH3 is limited to 1.2 Tbps. (297317)
- Layer2 source MAC learning may occur on packets received with CRC errors. (325507)
- Routed unicast traffic egressing a SVI for which destination MAC is not learnt are sent to CPU and then flooded on the egress VLAN. (368228)
- When 'hardware counter feature gre tunnel interface in' feature is enabled, the gre tunnel interface decap counters are not incremented when subinterface is used as the ingress interface. (464972)
- Per vlan routing and sub interface are not supported together. (486439)
- Grpc buffer-usage counters are not supported on Tomahawk3 platforms, and can cause forwarding agent crashes if configured (593626)

DCS-7050X, DCS-7250X and DCS-7300X Series

- Packets sourced from the CPU to be VXLAN encapsulated will not have the right DSCP marking in the outer header based on the global QOS map configuration. (139248)
- Tcam entries used by IPv6 standard access list is not shared across interfaces (159827)
- In MLAG VTEP configuration, the switch incorrectly drops VXLAN encapsulated packets that are destined to the VTEP IP address with the destination mac as peer switch's bridge MAC address. The workaround is to configure VARP in such scenarios. (173716)
- Multicast traffic destined to boundary or prefix mroutes configured may be forwarded out of order if fabric priority flow control is enabled for the given priority. (185981)
- If an SVI is used as a core interface to reach remote Vteps, any L3 EVPN traffic using that SVI will be dropped if the underlay mac becomes unlearnt. A workaround is to configure MAC timeout to a higher value than ARP timeout to ensure macs don't get aged out. (192419)

- During "reload hitless", ECMP traffic flows may get hashed to a different ECMP path than before the reload. (218700)
  Series Affected: DCS-7050X Series

- Direct flow on T2+ has the following limitations
  1. Only IP packets can have their source mac , destination mac and vlan changed.
  2. When a packet has its smac, dmac and vlan changed then it can only be forwarded to one interface.
  3. When a packet has its vlan changed it can only be forwarded untagged on access ports.
  4. An output interface must be specified whenever a packet's smac,dmac and/or vlan is changed. (251477)

- SFP+ and QSFP+ interfaces with a MAC loopback configuration (traffic-loopback or routing recirculation-interface) may erroneously allow the peer device to link up and blackhole traffic. To work around the issue, either unplug the cable or administratively shutdown the interface on the link partner. (494452)

DCS-7050X2 Series

- When IEEE 1588/PTP is configured on interfaces running at 100Mb/s speeds, the master offset and mean path delay calculations are inaccurate due to a limitation in the internal PHY (122816)

- Switch tries to perform VXLAN decapsulation of a packet if the destination IP of the packet matches the local Vtep IP address and the destination UDP port matches the configured VXLAN Port, even though the L2 Destination Mac address does not match any of its local Mac addresses. This can result in the packet getting dropped. This issue is more likely to be encountered when the switch happens to be an MLAG peer and the MLAG peers have the same VTEP IP configured. The MLAG switch may drop the received VXLAN encapsulated packets addressed to its MLAG peer's Mac address when the destination IP matches the shared VTEP IP configured on the MLAG Peers. (145099)
  Series Affected: DCS-7050SX2 Series

- Egress VLAN translation will not work on routed multicast packets when the VLAN to be translated is part of the outgoing interface list. (151093)

- VLAN translation is not supported on vxlan core ports (154309)
  Series Affected: DCS-7050X2 Series

- Due to an increase in the number of default entries programmed in the TCAM, 'Out of TCAM entries', might be seen while configuring ACLs. This happens due to the TCAM hardware resources being full. The workaround is to unconfigure any unused feature that requires TCAM resources. (182178)

- L2 protocol forwarding is not supported (470496)

Transceiver Series

- SFP-1G-T transceivers can only advertise one speed at a time. Desired speed and negotiation must be explicitly configured. Recommended commands are:

  * "speed auto" / "speed auto 1gfull" / "speed auto 1000full" : enable autoneg, advertise only 1G
  * "speed auto 100full" : enable autoneg, advertise only 100M
  * "speed 100full" : disable autoneg, force speed to 100M (159401)
  SKUs Affected: 1000BASE-T

- 25G transceivers could suffer signal degradation when using the MAM1Q00A-QSA QSFP-to-SFP adapter.

  Use a MAM1Q00A-QSA28 QSFP28-to-SFP28 adapter instead. (253324)

- For SKUs CAB-O-2Q-400G, CAB-O-4Q-400G, CAB-D-2Q-400G and CAB-D-4Q-400G, when operating at 25G or 50G NRZ speeds, forward error-correction should be manually configured (enabled or disabled) on both sides of the link as the default error-correction on both ends may not match. (392124)

- Revision 20 OSFP-400G-2FR4 transceivers may not correctly report the operational value of the configured Tx Input Equalization. This can be observed in 'show interfaces transceiver tuning detail', in which the Operational Tx Input Equalization may not match the Configured value. If the 'Tx Input Equalization' Configured column shows auto, automatic Tx Input Equalization is enabled, despite the Operational value shown. (423045)
  SKUs Affected: OSFP-400G-2FR4

- There is a hardware incompatibility between 100G AOCs with serial numbers starting with "AEB" and certain Mellanox adapters.

  The recommendation is to RMA for AOCs with serial numbers that don't start with "AEB". (457261)

- Interfaces with BCM82391 PHY do not support 1000BASE-T transceivers. (535121)

- QSFP200 cables and optics encoded using the CMIS specification are not recognized in QSFP100 ports. (536318)

- Active copper cables ACC-O-4QN-400 and ACC-D-4QN-400 incorrectly advertise autonegotiation capability.
  Only forced speeds are supported on these cables. (595191)
  SKUs Affected: ACC-D-4QN-400 and ACC-O-4QN-400

7300X3, CCS-720XP and DCS-7050X3 Series

- The DirectFlow "set vlan action" command is not supported. (237046)
- When configuring a DirectFlow action, specifying "interface hardware-loopback" as the destination of "action output" is not supported. (243031)
- IPv6 packets with WESP payload (next header 141) bypass the IPv6 security ACLs and service policies. (243387)
- Cut-through mode is not supported on SFP+ interfaces. (252731)
- Directflow configuration with "set vlan", but no "action set output interface" configured is not supported. (345852)
- NAT is not supported on subinterfaces (353236)
  SKUs Affected: 7300X3-32C-LC, 7300X3-48YC4-LC, DCS-7050CX3-32S and DCS-7050SX3-48YC12
- The following DirectFlow configurations are not supported: match input interface hardware-loopback
  action output interface <> (more than one)
  action output interface hardware-loopback
  action output flood|all
  action set cos (355927)
- Setting the default CoS value for a phone VLAN, using the CLI "switchport default phone vlan cos <>", takes effect only if the phone trunk port is in CoS trusted mode. If the phone trunk port is in CoS untrusted mode, then the port's default CoS value will be used for the phone VLAN. (390588)
- MAC Egress ACL configurations matching IP packets may not work when the IPv4/v6 per-interface counter feature is also configured. (411243)
- Leaf stateful switch upgrade is not supported on this platform. (415340)
  SKUs Affected: DCS-7050CX3M-32S-F and DCS-7050CX3M-32S-R
- CLI output of "show platform trident l3 shadow mpls-vc-and-swap-label" will show push
  as MplsLabelAction even for swap operation. (416134)
- MPLS packet undergoing swap operation does not honor the MTU configured on ingress/egress interface. (422668)
- Only 2K MPLS routes are supported (425691)
  Series Affected: CCS-720XP Series
- If the packet ingresses on one line card and egresses on a different line card, then a truncated egress mirrored packets will be 4 bytes shorter than

expected. (445200)
SKUs Affected: DCS-7304 and DCS-7308

- Dynamic NAT requires the forwarding table partition to be configured in flexible mode and entries allocated for exact-match table.
  Eg: platform trident forwarding-table partition flexible exact-match 49152 l2-shared 32768 l3-shared 131072
  If not configured, no logs or notification will be generated, and NAT might not work. (494088)

- NAT is not supported with non-default VRF. Configuring NAT over non-default VRF might cause Nat agent to restart continuously.

  Workaround is to remove the unsupported configuration. (499723)

- When IPV6 VXLAN underlay core interface is an access port on a SVI, VXLAN encapsulated packets may be sent out with VLAN tag in the outer ethernet header. The work around is to configure the port as a trunk port. (533929)

- "Dont fragment" bit is not set in the outer IP header of the VXLAN encapsulated packets when the payload is non-IP. (605003)

- When Postcard Telemetry is enabled, EVPN Multicast will not be supported. (614072)
  Series Affected: 7300X3, CCS-720XP, DCS-7050SX3, DCS-7050TX3 and DCS-7050X3 Series

DCS-7160 Series

- If there is a port ACL (PACL) or router ACL (RACL)
  that matches on L4 information for TCP/UDP/ICMP, and if the incoming packet has
  IP options, then those packets are dropped. (172932)

- No support for matching on DSCP field on IP packets for security ACLs. (174114)

- If the MAC address of the next-hop to reach a remote VTEP is not learned, and if the remote VTEP is configured for Head End Replication (HER) for a VXLAN VLAN, then, the the VTEP is not included in the list of HER VTEPs and no VXLAN BUM packets will be sent to that VTEP. The VTEP is included in the list of HER VTEPs once the underlay MAC address of the next-hop to reach that VTEP is learned.

  The workaround is to ensure that the underlay MAC of the next-hop to reach remote VTEPs are always present (which is the normal operation). (178395)

- Control plane Policy Map counters are not supported. (180303)

- A maximum of 3840 remote VTEPS are supported when the switch is configured as a Vxlan Vtep. (188553)
- Any IPv6 ACL containing a rule with the first 96 bits set as 0 cannot be configured when the algomatch profile is being used. (218453)
- Customer may witness around 100 milliseconds of packet loss when VxLAN ECMP nexthop changes. (219888)
- There may be traffic loss of up to 100 milliseconds when a VxLAN nexthop (as part of
  ECMP)undergoes modifications. (268600)
- The DSCP value of BGP control plane packets set by the command 'bgp transport qos
  dscp <value>' is overwritten when 'qos rewrite dscp' is enabled and the outgoing
  routed interface is a SVI. The rewritten value is based on traffic-class to DSCP
  map configuration. (288617)
- If a different XP profile than the one that is currently running is configured, and ACL
  configuration/ACL viewing commands without running a chip reset/reboot (via platform xp xp0 reset),
  the command can cause XpAcl to restart. (418083)
- VLAN ID match in IP ACLs is not supported on DCS-7160 platforms. (514366)
- If an incoming non-routable VXLAN-encapsulated packet is decap-eligible, but the encapsulation does not conform to VARP VTEP - VARP MAC binding, the packet will not be dropped and will continue to be switched based on the inner packet header. The impact is limited to extra or duplicate packets in the destination bridging domain, and does not affect packet forwarding correctness. However, it indicates an issue with the sender switch which is potentially generating illegal VXLAN-encapsulated packets. (562335)

Conditions and Impacts

The release notes listed above use shorthand terminology to refer to conditions that arise frequently in connection with bugs. This section explains each condition and its impact in more detail.

Condition: Rib agent restart
Impact: When the Rib agent goes down, all routing sessions are terminated; all BGP sessions drop, all OSPF adjacencies are lost, and neighbors stop forwarding traffic to us. When the Rib agent restarts, adjacencies are re-formed, and, after protocol convergence, traffic flows through us again. In most cases where there is adequate network-level redundancy, application-visible impact should be minimal

Condition: Rib agent hang
Impact: When the Rib agent hangs, routing protocols stop running. Routing peers will generally time out their session with the hung Rib agent, withdrawing routes accordingly. Meanwhile, the device continues to forward packets based on existing routing state. During this time, the device will not respond to routing topology changes. After a heartbeat timer expires (typically 10 minutes), the Rib agent restarts. In networks with sufficient redundancy, application impact of a Rib agent hang is usually low, because there is no data path disruption. However, in conjunction with other network changes (such as link failure or introduction), routing loops may occur.

Condition: kernel crash
Impact: A kernel crash has impact similar to issuing the "reload now" command. All links go down and all forwarding stops. Then, the system reloads, which may take up to 15 minutes. In a network with adequate redundancy, there should be minimal traffic loss associated with this period. After reload, links come up and protocols (LACP, STP, BGP, etc) reconverge. Protocol reconvergence is not necessarily hitless, depending on topology and configuration. For example, a switch may advertise a prefix to a connected subnet before STP has converged. However, any associated outage should be short lived, typically lasting around 30 seconds. The MLAG-SSO feature can dramatically reduce the window of disruption.

Condition: forwarding agent restart
Impact: A forwarding agent restart typically results in the switch ASIC being reset. It clears packet memory, dropping all packets currently in the switch, and causes all links to go down. The restart can take up to 45 seconds, during which time all links are down. Once the restart completes, all links come back up automatically, followed by protocol reconvergence (MLAG, LACP, STP, BGP/OSPF/IS-IS, etc). Depending on which protocols and options are in use, the reconvergence may take a few seconds up through several minutes. On modular switches, the impact of forwarding agent restart is limited to the affected line card; that is, if the forwarding agent for line card 3 restarts, then all ports on line card 3 bounce and protocols on those ports reconverge, but ports on other line cards are unaffected.