

Arista Networks EOS 4.24.1 Release Notes

Version: 1.3

24 June 2020

Table of Contents

EOS 4.24.1 Release Highlights

New Platforms and Hardware

SNMP MIBs

SNMP Traps

Supported Hardware

Reference to MLAG ISSU Upgrade/Downgrade Table

Enhancements in 4.24.1

Layer 3

Multi-agent

Layer 2

Layer 1

MPLS

General

Multicast

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

DCS-7280R and DCS-7500R Series

DCS-7280R3 and DCS-7500R3 Series

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

CCS-720XP Series

7368 Series

BGP EVPN L2/L3 VXLAN/MPLS

Resolved Caveats in 4.24.1

Layer 3

Multi-agent

Rib

Layer 2

Layer 1

CVX

General

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

DCS-7280R2 and DCS-7500R2 Series

DCS-7280R and DCS-7500R Series

DCS-7020RA, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards Series

DCS-7280R3 and DCS-7500R3 Series

DCS-7160 Series

DCS-7170 Series

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

DCS-7260X3 Series

DCS-7050CX3, DCS-7050SX3 and DCS-7300 Series

7368 Series

CCS-720XP Series

vEOS Router Series

BGP EVPN L2/L3 VXLAN/MPLS

Known Software Caveats in 4.24.1

Layer 3

Multi-agent

Rib

Layer 2

Layer 1

MLAG

Accelerated System Update

CVX

MPLS

General

Multicast

DCS-7150 Series

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

DCS-7280R and DCS-7500R Series

DCS-7020 Series

DCS-7020RA, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards Series

DCS-7280R3 and DCS-7500R3 Series

DCS-7280E and DCS-7500E Series

DCS-7160 Series

DCS-7170 Series

DCS-7170 Series

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

DCS-7050X2 and DCS-7300 Series

DCS-7010T Series

DCS-7060X and DCS-7300 Series

DCS-7050 and DCS-7300 Series

DCS-7260X3 Series

DCS-7050CX3, DCS-7050SX3 and DCS-7300 Series

7368 Series

CCS-720XP Series

DCS-7050X and DCS-7300 Series

DCS-7300 and DCS-7500 Series

DCS-7020RA, DCS-7160, DCS-7170, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards Series

Containerized EOS Series

Transceiver Series

vEOS Router Series

BGP EVPN L2/L3 VXLAN/MPLS

Limitations and Restrictions in 4.24.1

Layer 3

Multi-agent

Rib

Layer 2

Layer 1

MLAG

Accelerated System Update

CVX

MPLS

General

Multicast

DCS-7150 Series

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

DCS-7280R and DCS-7500R Series

DCS-7020 Series

DCS-7280R3 and DCS-7500R3 Series

DCS-7160 Series

DCS-7170 Series

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

DCS-7050X2 and DCS-7300 Series

DCS-7010T Series

DCS-7060X and DCS-7300 Series

DCS-7260X3 Series

DCS-7050CX3, DCS-7050SX3 and DCS-7300 Series

7368 Series

CCS-720XP Series

DCS-7050X and DCS-7300 Series

DCS-7300 and DCS-7500 Series

DCS-7020RA, DCS-7160, DCS-7170, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards Series

Transceiver Series

vEOS Router Series

BGP EVPN L2/L3 VXLAN/MPLS

Conditions and Impacts

EOS 4.24.1 Release Highlights

New Platforms and Hardware

- 7368-4D
- 7368-4P
- 7500R3-24D-LC
- CCS-720XP-96ZC2-F
- DCS-7050SX3-96YC8-F
- DCS-7050SX3-96YC8-R
- DCS-7280CR3MK-32D4-F
- DCS-7280CR3MK-32D4-R
- DCS-7280CR3MK-32P4-F
- DCS-7280CR3MK-32P4-R
- FAN-7012H-BLUE
- FAN-7012M-BLUE
- FAN-7012M-RED

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
- 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-F | • DCS-7280SR2-48YC6-R | • DCS-7050TX-64-F |
| • DCS-7170-64C-R | • DCS-7020TR-48-F | • DCS-7050TX-64-R |
| • DCS-7170-32C-F | • DCS-7020TR-48-R | • DCS-7050TX-64-SSD-F |
| • DCS-7170-32C-M-F | • DCS-7280QRA-C36S-F | • DCS-7050TX-64-SSD-R |
| • DCS-7170-32C-M-R | • DCS-7280QRA-C36S-R | • DCS-7050TX-72-SSD-F |
| • DCS-7170-32C-R | • DCS-7280SR2A-48YC6-F | • DCS-7050TX-72-SSD-R |
| • DCS-7170-64C-M-F | • DCS-7280SR2A-48YC6-M-F | • DCS-7050TX-96-SSD-F |
| • DCS-7170-64C-M-R | • DCS-7280SR2A-48YC6-M-R | • DCS-7050TX-96-SSD-R |
| • DCS-7170-32CD-F | • DCS-7280SR2A-48YC6-R | • DCS-7010T-48-F |
| • DCS-7170-32CD-R | • DCS-7280SRA-48C6-F | • DCS-7010T-48-R |
| • PWR-1100AC-F | • DCS-7280SRA-48C6-M-F | • DCS-7050SX-72-F |
| • PWR-1100AC-R | • DCS-7280SRA-48C6-M-R | • DCS-7050SX-72-R |
| • PWR-750AC-F | • DCS-7280SRA-48C6-R | • DCS-7050SX-72-SSD-F |
| • PWR-750AC-R | • DCS-7280TRA-48C6-F | • DCS-7050SX-72-SSD-R |
| • PWR-500-DC-F | • DCS-7280TRA-48C6-M-F | • DCS-7050SX-96-F |
| • PWR-500-DC-R | • DCS-7280TRA-48C6-M-R | • DCS-7050SX-96-R |
| • PWR-500AC-F | • DCS-7280TRA-48C6-R | • DCS-7050SX-96-SSD-F |
| • PWR-500AC-R | • DCS-7020TRA-48-F | • DCS-7050SX-96-SSD-R |
| • PWR-745AC-F | • DCS-7020TRA-48-R | • DCS-7050TX-128-SSD-F |
| • PWR-745AC-R | • DCS-7280CR2A-60-F | • DCS-7050TX-128-SSD-R |
| • FAN-7010 | • DCS-7280CR2K-60-F | • DCS-7050TX-72-F |
| • PWR-1900-DC-F | • DCS-7280SRAM-48C6-F | • DCS-7050TX-72-R |
| • PWR-1900-DC-R | • DCS-7280SRAM-48C6-R | • DCS-7050TX-96-F |
| • PWR-1900AC-F | • DCS-7280CR2-60-F | • DCS-7050TX-96-R |
| • PWR-1900AC-R | • DCS-7280CR2A-30-F | • DCS-7010T-48-DC-F |
| • PWR-747AC-F | • DCS-7280CR2K-30-F | • DCS-7010T-48-DC-R |
| • PWR-747AC-R | • DCS-7280QRA-C36S-M-F | • DCS-7260QX-64-F |
| • FAN-7002H-R | • DCS-7280QRA-C36S-M-R | • DCS-7260QX-64-R |
| • FAN-7000H-R | • DCS-7280SR2K-48C6-M-F | • DCS-7260QX-64-SSD-F |
| • PWR-1600AC-F | • DCS-7280SR2K-48C6-M-R | • DCS-7260QX-64-SSD-R |
| • FAN-7001D-F | • DCS-7020SR-24C2-F | • DCS-7050SX-72Q-F |
| • FAN-7001C-F | • DCS-7020SR-24C2-R | • DCS-7050SX-72Q-R |
| • PWR-400AC-BLUE | • DCS-7280CR2M-30-F | • DCS-7050TX-72Q-F |
| • FAN-7011M-F | • DCS-7280SRM-40CX2-F | • DCS-7050TX-72Q-R |
| • FAN-7011M-R | • DCS-7280SRM-40CX2-R | • DCS-7050QX2-32S-F |
| • PWR-1021-AC-RED | • DCS-7020SR-32C2-F | • DCS-7050QX2-32S-R |
| • PWR-511-AC-BLUE | • DCS-7020SR-32C2-R | • DCS-7050SX2-128-F |
| • PWR-511-AC-RED | • DCS-7020SRG-24C2-F | • DCS-7050SX2-128-R |

- PWR-621-AC-RED
- PWR-400AC-RED
- FAN-7001DH-F
- PWR-1611-AC-RED
- PWR-1611-DC-RED
- 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-F
- FAN-7000-R
- PWR-460AC-F
- PWR-460AC-R
- PWR-460DC-F
- PWR-460DC-R
- DCS-7280CR-48-F
- DCS-7280QR-C36-F
- DCS-7280QR-C36-M-F
- DCS-7280QR-C36-M-R
- DCS-7280QR-C36-R
- 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-F
- DCS-7280QR-C72-M-F
- DCS-7280QR-C72-M-R
- DCS-7020SRG-24C2-R
- DCS-7280CR3-32P4-F
- DCS-7280CR3-32P4-M-F
- DCS-7280CR3-32P4-M-R
- DCS-7280CR3-32P4-R
- DCS-7280CR3K-32P4-F
- DCS-7280CR3K-32P4-R
- DCS-7280CR3-32D4-F
- DCS-7280CR3-32D4-M-F
- DCS-7280CR3-32D4-M-R
- DCS-7280CR3-32D4-R
- DCS-7280CR3K-32D4-F
- DCS-7280CR3K-32D4-R
- DCS-7280PR3-24-F
- DCS-7280PR3-24-M-F
- DCS-7280PR3K-24-F
- DCS-7280DR3-24-F
- DCS-7280DR3-24-M-F
- DCS-7280CR3-96-F
- DCS-7280CR3K-96-F
- DCS-7280CR3MK-32P4-F
- DCS-7280CR3MK-32P4-R
- DCS-7280DR3K-24-F
- DCS-7280CR3MK-32D4-F
- DCS-7280CR3MK-32D4-R
- DCS-7050SX-128-F
- DCS-7050SX-128-R
- DCS-7050SX-128-SSD-F
- DCS-7050SX-128-SSD-R
- DCS-7250QX-64-F
- DCS-7250QX-64-R
- DCS-7250QX-64-SSD-F
- DCS-7250QX-64-SSD-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-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-7050TX2-128-F
- DCS-7050TX2-128-R
- DCS-7050SX2-72Q-F
- DCS-7050SX2-72Q-R
- DCS-7060CX-32S-F
- DCS-7060CX-32S-R
- DCS-7060CX2-32S-F
- DCS-7060CX2-32S-R
- DCS-7260CX-64-F
- DCS-7260CX-64-R
- DCS-7260CX-64-SSD-F
- DCS-7260CX-64-SSD-R
- DCS-7060SX2-48YC6-F
- DCS-7060SX2-48YC6-R
- DCS-7260CX3-64-F
- DCS-7260CX3-64-R
- DCS-7050CX3-32S-F
- DCS-7050CX3-32S-R
- DCS-7050SX3-48YC12-F
- CCS-720XP-24ZY4-F
- CCS-720XP-48ZC2-F
- DCS-7050SX3-48YC8-F
- DCS-7050SX3-48YC8-R
- DCS-7260CX3-64E-F
- DCS-7260CX3-64E-R
- DCS-7060DX4-32-F
- DCS-7060PX4-32-F
- CCS-720XP-24Y6-F
- CCS-720XP-48Y6-F
- DCS-7050CX3M-32S-F
- DCS-7050CX3M-32S-R
- CCS-720XP-24Y6-R
- CCS-720XP-48Y6-R
- DCS-7050SX3-48C8-F
- DCS-7050SX3-48C8-R
- DCS-7050TX3-48C8-F
- DCS-7050TX3-48C8-R
- CCS-720XP-96ZC2-F
- DCS-7050SX3-96YC8-F
- DCS-7050SX3-96YC8-R
- DCS-7160-32CQ-F
- DCS-7160-32CQ-R
- DCS-7160-48YC6-F
- DCS-7160-48YC6-R
- DCS-7160-48TC6-F
- DCS-7160-48TC6-R
- FAN-7002-F

- DCS-7280QR-C72-R
- DCS-7280SR2-48YC6-F
- DCS-7280SR2-48YC6-M-F
- DCS-7280SR2-48YC6-M-R
- DCS-7050TX-48-F
- DCS-7050TX-48-R
- DCS-7050TX-48-SSD-F
- DCS-7050TX-48-SSD-R
- FAN-7002-R
- FAN-7002H-F
- FAN-7000H-F

Modular

- FAN-7002-F
- FAN-7002-R
- FAN-7002H-F
- FAN-7000H-F
- PWR-3K-AC-F
- PWR-3K-AC-R
- PWR-2700-DC-F
- PWR-2700-DC-R
- PWR-3K-DC-BLUE
- PWR-3K-DC-RED
- PWR-3KT-AC-BLUE
- PWR-3KT-AC-RED
- PWR-D1-3041-AC-BLUE
- PWR-2900AC
- DCS-7500E-SUP
- DCS-7500E-SUP-D
- 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
- 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
- 7508R3-FM
- 7500R3K-36CQ-LC
- 7500R3-24P-LC
- 7800R3-36P-LC
- 7800R3-48CQ-LC
- 7800R3-48CQM-LC
- 7800R3K-48CQ-LC
- 7808R3-FM
- DCS-7800-SUP
- DCS-7808-CH
- 7804R3-FM
- DCS-7804-CH
- 7500R3-24D-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
- 7324X-FM
- 7328X-FM
- 7300X3-32C-LC
- 7304X3-FM
- 7308X3-FM
- 7300X3-48YC4-LC
- 7368
- 7368-16C
- 7368-SUP
- 7368-SUP-D
- 7368X4-SC
- 7300-SUP2-D
- 7368-4D
- 7368-4P

Transceiver

- 1000BASE-BX10-D
- 1000BASE-BX10-U
- 40GBASE-AOC
- 10GBASE-LRL
- 10GBASE-ZR
- 40GBASE-PLRL4
- 40GBASE-SR4
- 40GBASE-XSR4
- 25GBASE-CR
- 25GBASE-LR
- 25GBASE-SR
- 100GBASE-SRBD
- 100GBASE-SWDM4
- 100GBASE-ERL4
- 100GE-DWDM2
- CFP2-100G-DWDM-DCO
- CAB-D-4Q-400G
- CAB-D-8S-200G
- CAB-D-D-400G
- CAB-O-2Q-200G
- CAB-O-2Q-400G
- CAB-O-4Q-200G
- CAB-O-4Q-400G
- CAB-O-8S-200G

- 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
- 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-D
- 10GBASE-ERBD-U
- 10GBASE-ERLBD-D
- 10GBASE-ERLBD-U
- ADPT-O-Q-100G
- AOC-D-D-400G
- AOC-O-O-400G
- CAB-D-2Q-200G
- CAB-D-2Q-400G
- CAB-D-4Q-200G
- CAB-O-O-400G
- OSFP-400G-2FR4
- OSFP-400G-LR8
- OSFP-400G-SR8
- QDD-400G-LR8
- QDD-400G-SR8
- 100GBASE-FR
- CAB-Q-2Q-100G
- OSFP-400G-DR4
- 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-XDR4
- 10GBASE-ER
- 40GBASE-CR4

Reference to MLAG ISSU Upgrade/Downgrade Table

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

Enhancements in 4.24.1

Layer 3

- Support for LDP Graceful Restart (296115)
- Hardware BFD J2 support (414559)
- Added support for protection of IS-IS SR anycast segments using TI-LFA (431058)
- Add the support to introduce Name and Description as configurable attributes for Segment-Routing policies. (452193)
- Hardware BFD support (463721)
Series Affected: 7368 Series

Multi-agent

- The "show ip bgp neighbors" and "show ipv6 bgp peers" commands have been enhanced to show the best path statistics as part of the prefix statistics. (298233)
- Support for BGP Accumulated IGP Metric (RFC 7311) in IPv4 and IPv6 Unicast address families (339477)
- Support for up to 64 AS numbers in Route Map as-path "prepend", "last-as" and "match all replacement" in multi-agent mode (346596)
- Support for regenerating BGP link-bandwidth extended community values towards eBGP peers using outbound policy (379733)
- Hitless Bgp agent restart support for IPv4 and IPv6 unicast address families (385719)
- Support for redistributing connected, static and IS-IS routes into OSPFv3 in the target VRF (409856)
- Added Eos Sdk support of iterating IPv4 Unicast and IPv6 Unicast Bgp Adj-Rib-In paths (429236)
- Added support to show time since last update (age) for the routes in 'show rib route ip[v6]' (439004)
- Support for switching to backup via when the IGP route resolving the primary BGP next hop gets deleted. (444569)
- Added support for steering BGP MPLS VPN, L3EVPN, EVPN VPWS, and 6PE traffic over SR-TE policies. (455782)
- Phase-1 support for Routing Control Functions (457774)

Layer 2

- Reduce inadvertent STP timeouts in busy systems. (276927)
- Introducing "show mac security profile" command display MACsec profiles (423200)
- EOS SDK now supports iterating over configured MacSec profiles. (424735)

Layer 1

- Support auto-negotiation for 25G, 40G, 50G (2 lane), 50G (1 lane), 100G (4 lane), 100G (2 lane), 200G and 400G speeds. (412955)
Series Affected: DCS-7060X4 Series
- Added support for MACsec (463699)
SKUs Affected: DCS-7280CR3MK-32P4-F and DCS-7280CR3MK-32P4-R
- On interfaces with a CMS42550 phy, display Fire-Code FEC counters in the "show interface phy detail" CLI command. (464206)

MPLS

- Support for MPLS static tunnel ECMP (433662)

General

- Added support for the SNMP inetCidrRouteTable. (6094)
- Support for CALEA operators and Legal Intercept operations (372210)
- Support for DHCP Vendor Option with sub-options (DHCP option 43) in DHCPv4. (414044)
- If the CLI 'dot1x timeout reauth-timeout-ignore always' is configured and AAA reauthentications occur when the RADIUS server is down, then, dot1x clients will continue to use the RADIUS attributes received for the last successful authentication. (419831)
- Add support for configurable system MAC address on fixed systems. (445233)
Series Affected: DCS-7010, DCS-7010T, DCS-7050, DCS-7050CX3, DCS-7050Q, DCS-7050S, DCS-7050SX2, DCS-7050SX3, DCS-7050T, DCS-7050TX, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060CX, DCS-7060CX2, DCS-7060SX2, DCS-7060X, DCS-7060X2, DCS-7060X3, DCS-7060X4, DCS-7150, DCS-7160, DCS-7170, DCS-7250X, DCS-7260CX, DCS-7260CX3, DCS-7260QX, DCS-7260X, DCS-7260X3, DCS-7280CR2, DCS-7280E, DCS-7280R, DCS-7280R2, DCS-7280SE, DCS-7280SR, DCS-7280SR2 and DCS-7280TR Series

- Authorization may now be configured for OpenConfig gNMI connections, by specifying 'authorization requests' in the 'transport grpc <name>' mode. This allows for per-RPC authorization. (445861)
- EOS-SDK support for MACsec Profile CLI - "key retirement immediate". (450587)
- "aaa unresponsive action traffic allow [vlan <vlanID>]" is a new knob that, when enabled, makes EOS assign a user to the provided VLAN (or to the native VLAN) when his authentication is unable to complete because the AAA server is unreachable or times out. (467177)

Multicast

- Support to delay installing (S, G) routes in the hardware until its data traffic is seen (447802)

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

- Support for packet counters without byte counters in hardware counter features for ingress ACLs and egress IPv6 ACLs. (356388)
- Support matching of source and destination port ranges with the STCP protocol in ACL features including policy-map (447278)
Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- Added the CLI command 'inactive mac-address destination peer-link [direct | indirect]' under the mlag configuration mode to explicitly override whether or not fast MAC redirection is enabled. (450550)
- Support for DSCP masks in IPv6 port ACLs (464020)
- Support VRF matching in DirectFlow (470301)
Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

DCS-7280R and DCS-7500R Series

- Support OSPFv2 over GRE tunnel interfaces. (421345)
- Support appending a new FCS on every frame after the original FCS while in TAP Aggregation mode (435055)
- Support OSPFv2 over GRE tunnel interfaces (444767)
- Support mirroring action in egress MAC ACL (445988)
- Support metadata reporting for Tx mirrored packets when the mirroring destination is a GRE tunnel. (455906)

DCS-7280R3 and DCS-7500R3 Series

- Support CPU traffic policies for 7500R3 and 7280R3 platforms (292695)
- Add support for configuration of two serdes rates per speed group. (417502)
- Support for SR-TE CBF (421171)
- Support for VXLAN overlay Multicast forwarding using underlay multicast tree. (427205)
- Support for Qos policies on SVIs. (436344)
- Added BGP Flowspec support on DCS-7500R3 and DCS-7280R3. (444942)
- Support for multiple sFlow collectors with hardware accelerated sFlow on Jericho2 (449808)
- Support Identity tagging with up to two Dot1Q tags, and Dot1Q tags stripping for up to two tags, while in Tap Aggregation mode (452943)
- Egress IPV4 and IPV6 per-interface counters are now supported. (458749)
- Support for 1K VRFs (459968)
- Display corrected symbol rate count in the "show interfaces phy detail" CLI command. (463741)
- Support for two rate, three color meters (TrTcm) QoS policers. (469976)

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

- On platforms that support per-priority PFC counters, a syslog will be emitted to monitor Rx PFC frames that are received on priorities which are not configured to honor PFC. (222184)
- Support for Fast Poll Counters. (289994)
- Add support for Stateful Switchover on 7300X3-32C-LC and 7300X3-48YC4-LC linecards. (342067)
SKUs Affected: 7300X3-32C-LC and 7300X3-48YC4-LC
- Support for Transient Capture Buffer feature (343738)
Series Affected: DCS-7050X3 Series
- Support for IPv6 multicast route counters per group, source and vrf. (346834)
- Improve scale for static NAT with filter, when large access-lists are used, or the access-lists are shared by multiple NAT rules: "hardware nat static

access-list resource sharing". (366880)

Series Affected: CCS-720XP and DCS-7050X3 Series

- Added support for aggressive linkup CLI (423076)
Series Affected: DCS-7010, DCS-7050TX, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060CX, DCS-7060CX2, DCS-7060SX2, DCS-7260CX3 and DCS-7260QX Series
SKUs Affected: 7300X-64S-LC, 7300X-64T-LC, 7300X3-48YC4-LC, CCS-720XP-24Y6-F, CCS-720XP-24Y6-R, CCS-720XP-24ZY4-F, CCS-720XP-48Y6-F, CCS-720XP-48Y6-R, CCS-720XP-48ZC2-F, DCS-7050TX2-128-F, DCS-7050TX2-128-R, DCS-7050TX3-48C8-F and DCS-7050TX3-48C8-R
- Added support for aggressive linkup CLI (447567)
SKUs Affected: DCS-7060DX4-32-F and DCS-7060PX4-32-F
- Support for the "show platform trident egress event debug" CLI command, which outputs egress pipeline events that have hit on the ASIC. (471436)

CCS-720XP Series

- Support for CCS-720XP-96ZC2 (389158)

7368 Series

- Software support for 7368-4D (336885)
SKUs Affected: 7368-4D
- Software support for 7368-4P. (352372)
SKUs Affected: 7368-4P
- Support for GRPC interface and subinterface counters. (372391)
- Enable egress sflow sampling. (424509)
- MPLS pop action supports IPv4/IPv6 and MPLS payload. (458798)

BGP EVPN L2/L3 VXLAN/MPLS

- Added support for IPv6 underlay for Vxlan (339801)

Resolved Caveats in 4.24.1

Layer 3

- When layer 3 forwarding agent is restarted, it is possible that the agent does not reach warm state. The workaround is to restart the agent again, the second restart may cause traffic loss. (435193)
- When a static ARP entry is added via CLI with a MAC of 0.0.0, Arp will continuously crash. The workaround is to either remove the static ARP entry or add a non zero MAC address to the static ARP entry. (444677)

- With FIB compression being enabled, the StrataL3 agent and SandL3Unicast agent can restart unexpectedly. (445777)
- IPv6 Egress ACLs may not be applied to traffic if 'ip hardware fib next-hop sharing' is also configured (446000)
- OSPF may incorrectly originate an Indication LSA in an area which has LSAs with the DC-bit cleared. (458064)
- When using OSPFv3 and encryption or OSPFv2 and encryption, the Rib agent may stop responding and restart unexpectedly. (472846)
- When Policy Based Routing is enabled, packets destined to the switch but also matching the PBR policy, may get redirected by PBR policy. (473529)
 Series Affected: 7300X3, 7320X, 7368, CCS-720XP, DCS-7010, DCS-7010T, DCS-7050, DCS-7050CX3, DCS-7050Q, DCS-7050S, DCS-7050SX2, DCS-7050SX3, DCS-7050T, DCS-7050TX, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060CX, DCS-7060CX2, DCS-7060SX2, DCS-7060X, DCS-7060X2, DCS-7060X3, DCS-7060X4, DCS-7250X, DCS-7260CX, DCS-7260CX3, DCS-7260QX, DCS-7260X, DCS-7260X3, DCS-7300, DCS-7300X and DCS-7320 Series
- Running 'show ipv6 hardware ale routes <prefix>' with a prefix that has trailing bits that exceed the prefix length will cause the platform agent to restart. (473799)
- After several subsequent interface shut/no shut, some routes might not forward traffic. The workaround is to toggle the interface once more. (476768)
- Running the command 'no bfd neighbor ADDR' on a Port-Channel with BFD neighbors configured where "ADDR" is either an IPv4 or IPv6 address will result in the removal of all BFD neighbor configuration regardless of address-family. The work-around is to re-add the incorrectly-removed BFD neighbor configuration via the 'bfd neighbor' command. (477517)
- When the MAC address changes on a BFD peer, the session may flap. This can happen when the interface fails over from active to standby. (477559)
- Some nexthop group configuration changes may not be processed when nexthop group config is undergoing high churn. This can result in traffic loss for routes going over the nexthop groups. (480952)
- Routes being removed when they are churning from up to down states may lead to memory leaks. (481312)
- After performing a stateful switchover, the L3 platform agent may fail to warm up if some IP routes fail programming due to hardware resource overflow. (484049)

Multi-agent

- IS-IS SR LFIB may be deleted and recreated if the ECMP resolution for IS-IS SR adjacency segment changes (457220)
- Setting the retry interval and expire interval to the same value might cause Rpki agent to restart unexpectedly when the cache enters the disabled state. (461420)
- The RPKI agent will not properly sync ROAs after a stateful switchover. Issue 'clear bgp rpki cache all' to recover.

An event handler can be created that reacts to a switchover log message and triggers a 'clear bgp rpki cache all':

```
event-handler refresh-rpki
    action bash CliShell -p 15 -c 'wait-for-warmup Rpki' && CliShell -p 15 -
c 'clear bgp rpki cache all'
    asynchronous
    timeout 300
    !
    trigger on-logging
        regex REDUNDANCY-5-IS_ACTIVE (470933)
```

- Running "show bgp rpki cache [<cache name>] detail" or "clear bgp rpki cache (all|<cache name>) [counters]" commands while the Rpki agent is initializing might lead to Rpki agent restarting several times before stabilizing. (470961)
- Dynamic Prefix List configuration on more than one VRF does not take effect (471072)
- An IPv6 unicast path may get invalidated for a peer that has both IPv6 unicast and 6PE negotiated, if the next hop is changed using an inbound route map. (471675)
- Configuring RPKI caches with different preferences is not supported. When a cache changes from Active to Idle due to a preference change, if it is in the progress of syncing this operation will be aborted but ROAs that it had previously synced are not properly cleaned up from the local table. (472296)
- The BGP agent can restart unexpectedly if it receives an RPKI prefix PDU with a max length less than the prefix length. (478027)
- In Multi-agent model, EosSdk ip route does not work as the route is set with invalid route type. (478236)

Rib

- The dynamic flooding algorithm to compute the flooding topology picks a start node to begin the computation. When that node is partitioned from the Area Leader, the nodes in the Area Leader's partition will not be in the flooding topology. This causes the problem of that partition being exposed to a congestive collapse. This problem lasts until the LSPs of the incorrect start node are timed out, which is typically 20 minutes but could be different if lsp refresh interval is configured).

Suggested workaround: To reduce the probability of this happening, prioritize the Area Leader to be the node with the highest degree of connectivity. Configuration statement:

```
arista(config-router-isis)#area leader priority ?
```

```
<0-255> Area leader priority
```

This workaround will not work in all situations since connectivity of a node will change and there may be multiple nodes with the same degree of connectivity. But it does reduce the probability of hitting this bug for a given topology. (429480)

- In the presence of tie breaker configuration for ECMP paths, the Rib agent may exit unexpectedly while handling BGP updates for a prefix having ECMP, when some paths of the given prefix are undergoing metric change. Workaround is to remove tie breaker configuration. (444000)
- In extremely rare circumstances when additional paths send any is enabled and a neighbor continuous route churn for same NLRI may trigger Rib restart (465132)

Layer 2

- ASU upgrade to florence-C1(4.22.4M) may fail at first attempt and succeed at next attempt. (461655)
- The IP source guard configuration on Port-Channels may not take into effect after system reboots or platform agent restarts. The workaround is to remove member ports from the Port-Channel and then add them back. (475478)

Layer 1

- Ingress packets may be dropped in the MACsec PHY. (450895)
SKUs Affected: 7500R2M-36CQ-LC, DCS-7280CR2M-30-F, DCS-7280SRAM-48C6-F, DCS-7280SRAM-48C6-R, DCS-7280SRM-40CX2-F and DCS-7280SRM-40CX2-R

CVX

- The Arista OpenStack plugin has been enhanced to create a default route for the routers created in OpenStack, when VRF creation and `vrf_default_route` option is enabled in the `networking-arista` plugin configuration (295274)
- When a group on NSX-T containing more than 1000 hosts, policy rules for the group on CVX will only generate ACLs for the first 1000 hosts in that group. (459644)
- The Policy Control Service (PCS) fails to apply any security policy configured on NSX-T on a switch interface after the switch configuration is modified to remove all tags from an interface followed by re-adding tags, using the configuration replace feature. (463958)

General

- Any update in OpenConfig removes the "shutdown" configuration from Management interfaces (250235)
- The ZeroTouch agent does not properly handle 301 HTTP return codes when downloading the bootstrap script. This can lead to the device leaving ZTP mode with a default startup-config. (342098)
- ZTP can stop cycling speeds on front-panel ports whose capabilities have no supported speeds for a possible speed-group configuration; this will not affect management ports. For example: a 40G-only transceiver inserted into a port with a default speed-group setting of 25G. (444861)
- Removing a bash action from an event-handler via "action bash" can result in inability to copy and paste that particular event-handler config. A workaround is to use "action bash :". (452832)
- Installing 64-bit rpm fails with 32-bit EOS.swi on older supervisors (457100)
- If any interface is configured with "ip address unnumbered", configuration changes made with gNMI, NETCONF, or RESTCONF do not apply.

To workaround the issue "ip address unnumbered" needs to be removed from the configuration via the CLI or EAPI. (457161)

- When the switch reloads, it might fail to mount the internal flash, entering Zero Touch mode. Going to bash and reload by running 'sudo reboot' will fix the problem. (460245)
- ISIS configuration on a non-default VRF via OpenConfig fails. (460407)

- Non-alphanumeric characters (with the exception of '-', '_', and '~') in VRF names may prevent some inter-process communication, resulting in some state not being updated in those VRFs. (464188)
- When configuring a VLAN_AWARE_BUNDLE evpn-instance via OpenConfig that contains a VLAN range and VLANs with ETIDs, the VLANs with ETIDs will not be retained. Only the VLAN range will apply. A work around is to configure the range first and follow with any VLANs with specific ETIDs. (470793)
- Removing a bash action from an event-handler via "action bash" can result in inability to copy and paste that particular event-handler config. A workaround is to use "action bash :". (471816)
- The VFAT flash filesystem can get corrupted after reload.

To recover, reload the system again. (471854)
- Under limited circumstances, telnet may behave in an unexpected manner (472113)
- When more than one DHCP server is configured with IP Locking, a host may experience packet drops for up to 150 seconds after leasing a second IP from one of the configured servers. (476860)
- Under certain circumstances flash may be remounted read-only if dosfsck was not able to fix FS corruption on first pass (481251)

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

- The loop protect feature does not work on ports of Algomatch enabled linecards and fixed systems. (361130)
- While in Tap Aggregation mode with VXLAN tags stripping feature enabled, forwarding of VXLAN tagged packets will be disrupted if the Sand agent or the SandFap agent restarts.

Reconfiguring the VXLAN tag stripping feature on the relevant tap ports will restore functionality. (372603)
- Flapping BGP Flowspec configuration on an interface where the neighbor is publishing large number of Flowspec matches may cause the forwarding agent to crash. (439838)
- IP multicast packets may get mis-routed in an MLAG configuration when the peer chassis is rebooted in a multi FAP system. A restart of the SandMcast agent will clear the left over entries from the hardware. (444856)

- With PIM enabled on a VXLAN SVI configuration, reload of a switch might lead to incorrect flooding of PIM packets to remote VTEPs, causing PIM neighborship to not form between the MLAG pair, leading to misforwarding of routed multicast traffic in overlay. "shut", "no shut" of SVI would resolve the issue. (445280)
- Priority Flow Control pause watchdog actions "errdisable" and "notify-only" actions are not supported. (450857)
- Interface-level Priority Flow Control (PFC) watchdog commands are not supported. (450860)
- If Flowspec is enabled on a subinterface and the Flowspec feature is using 'port qualifier size 1 bits' in the tcam profile configuration, all traffic coming into that physical port will be subject to the flowspec rules, including other subinterfaces and the parent interface. (453067)
- Flowspec configuration on a subinterface is not blocked when the Flowspec feature is using 'port qualifier size 1 bits' in the tcam profile configuration. (453068)
- When vlan-based "legacy" interface connector used in patch (pseudowire or local-local), and the connector references a port-channel interface, the patch may not become operational. Show patch panel will indicate patch is down. SandTunnel trace messages may indicate error allocating outAc Entry. (466176)
- When a link-down debounce timer is configured (link-debounce time <time> or link-debounce time 0 <time>), if, at the expiration of the debounce timer, the PCS is up but a LF is present the local link can be down but fail to send remote fault to the peer.
The workaround is to not use a link-down debounce. (471886)
- When vlan-based connector used in patch panel config (pseudowire or local-local), subinterfaces may remain in the down state due to outAc entry leakage. (471887)
- A packet egressing a QinQ subinterface could have its outer VLAN tag stripped.

A workaround is to restart the SandTopo agent. (473305)

- VxLAN terminated packets with inner IPv6 payload may be incorrectly subjected to IPv4 RACLs. (475953)

DCS-7280R2 and DCS-7500R2 Series

- IPv4 multicast routed traffic may be lost intermittently. Also, when a hardware parity error in the LEM table occurs, it may not be corrected by software leading to drops or mis-forwarding of multicast routed traffic and/

or IGMP snooped traffic. As well, if there is churn in multicast routes and/or IGMP snooping groups while the SandMcast agent is restarting, there may be a reduction in the scale of unicast MACs; IPv4 multicast routes; and/or IGMP snooping groups and unicast routes. (477646)

DCS-7280R and DCS-7500R Series

- BFD may briefly drop packets when the standby supervisor comes back online. (389057)
SKUs Affected: DCS-7504, DCS-7504N, DCS-7508, DCS-7508N, DCS-7512N and DCS-7516N
- PFC pause frames, if received on /3 subport of Sesto2 master ports, will not be honored on the affected platforms. (411352)
SKUs Affected: DCS-7280QR-C72-F, DCS-7280QR-C72-M-F, DCS-7280QR-C72-M-R, DCS-7280QR-C72-R, DCS-7280QRA-C36S-F, DCS-7280QRA-C36S-M-F and DCS-7280QRA-C36S-M-R

DCS-7020RA, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards Series

- With AlgoMatch enabled, the tc-counters TCAM profile applied, an IPv6 security ACL applied on an interface, and an IPv6 PBR policy applied on the same interface as the ACL, actions for that ACL (deny, count, etc) will not apply to incoming traffic. (399725)
- AlgoMatch ACLs are incorrectly applied to terminated Vxlan IPv6 traffic when using the vxlan-routing TACM profile. The following workaround can resolve the issue:
 - Create a copy of the vxlan-routing TCAM profile
profile vxlan-routing-copy copy vxlan-routing
 - Remove the packet type causing the issue
profile vxlan-routing-copy
feature acl port ip
no packet ipv4 vxlan eth ipv6 forwarding routed decap
exit
feature acl vlan ip
no packet ipv4 vxlan eth ipv6 forwarding routed decap
exit
 - Apply the new TCAM profile
system profile vxlan-routing-copy (460038)
- Traffic egressing out of a LAG interface may not be subject to egress ACL on reload (473227)

DCS-7280R3 and DCS-7500R3 Series

- Applying a Qos policy on Vlan interfaces may result in SandAcl restart, since this functionality isn't supported. (403280)
- Applying a Qos policy on sub-interfaces may result in SandAcl restart, since this functionality isn't supported. (403281)
- SandAegis agent may crash when the last IPv6 rule is deleted from a traffic-policy which has both IPv4 and IPv6 rules (435733)
- In some scenarios ECC 2-bit errors may not be software corrected. (439132)
- VXLAN IPv6 overlay configuration along with VARP and Virtual VTEP configuration is not supported. (442914)
- After switch reboot VxLAN encapsulation header may not get applied properly in the packet path. (461365)
- The command 'switchport tool identity' has no effect. Configured identity tags are always allowed to pass out of tool interfaces. (461493)
- While in TAP Aggregation mode, packets with destination MAC addresses in the range from xx:88:xx:xx:xx:xx to xx:8b:xx:xx:xx:xx, inclusive, may be dropped unconditionally. This issue is persistent and does not have an available workaround. (466628)
- Reloading a switch while in TAP Aggregation mode, or entering TAP Aggregation mode immediately after a switch is booted up, may prevent TAP Aggregation traffic forwarding.

Disable TAP Aggregation, restart the SandDanz feature agent using "[no] agent SandDanz shutdown", and then enable TAP Aggregation to restore functionality. (466730)

- MPLS packets with more than 10 labels, are not forwarded correctly. (467327)
- Some non-control packets might not get dropped as priority drop when the device ingress maximum packet rate is oversubscribed. (471513)
- BasicQos functionality may not work on system boot .Workaround is to restart SandTm agent after system boot is complete. (471630)
- When a traffic policy is applied on an interface, incoming packets with IPv4/IPv6 source/destination addresses not matching any source/destination prefix in the traffic policy applied on the interface may cause the packet processing pipeline to become unable to process incoming packets.

A workaround is to add to the end of each traffic policy an IPv4 match rule with source prefix 0.0.0.0/0 and destination prefix 0.0.0.0/0; in addition,

an IPv6 match rule with source prefix ::/0 and destination prefix ::/0. A restart of the SandFapNi slice agent(s) is required if packets are not forwarding. (475222)

SKUs Affected: 7500R3K-36CQ-LC, 7800R3K-48CQ-LC, DCS-7280CR3K-32D4-F, DCS-7280CR3K-32D4-R, DCS-7280CR3K-32P4-F, DCS-7280CR3K-96-F, DCS-7280DR3K-24-F and DCS-7280PR3K-24-F

- For a parent interface with multiple subinterfaces under it all with the same ipv6 PBR policy applied, if a subinterface is shutdown the policy no longer works for all of the subinterfaces under that parent. A workaround for this is to remove and re-attach the PBR policy on any subinterface. (477273)
- The listed ports cannot link up at 50G-2 speed.
DCS-7280CR3-96/DCS-7280CR3K-96: Port 3, 7, 11, 15, 19, 23, 27, 31, 35, 39
7800R3-48CQ-LC/7800R3K-48CQ-LC: Port 41-48 (478237)
SKUs Affected: 7800R3-48CQ-LC, 7800R3K-48CQ-LC, DCS-7280CR3-96-F and DCS-7280CR3K-96-F
- On system boot kernel interfaces may not get created.
As a workaround SandFapNi agent should be restarted. (478401)
- When 'set dscp' action is applied to ECN capable packet, and there is no ECN congestion experienced by the packet, the ECN bits of the packet get reset to 0. (482029)
- Linecard hotswap or a switch reboot when the traffic is running may cause all packets to drop at ingress of one or more forwarding chips. Restart of the SandFapNi agent instance for the affected chips will resolve the issue. (483181)

DCS-7160 Series

- Value of outer/underlay UDP source port of VXLAN encapsulated packet may vary based on overlay packet size for a given overlay packet flow (identical overlay/inner 5 tuple). This could lead to unnecessary ECMP load balancing of egress VXLAN encapsulated TCP packet which can further lead to performance issues for a overlay TCP session/flow. (422669)
- XpL2 crashing with VLANs configured on trunk ports can cause unexpected ingress VLAN translation, incorrect MAC learning, L2 loops, and possibly more, indefinitely.

Workaround is to remove and re-add the VLANs from the port's configuration, or unconfigure and reconfigure all VLANs, or reload. (475570)

- If incoming BFD packet is encapsulated by VXLAN and overlay Destination MAC address is router MAC then BFD packet may get dropped and BFD session state remains down (477801)

DCS-7170 Series

- Routing change can transiently cause a packet to take a shorter prefix route (393732)
- On DCS-7170 series, a policer configuration with burst unit in mbytes will result in continuous crash of BfnQos agent. Remove the configuration to recover, and the issue can be worked around by specifying the burst in kbytes. (469790)
- When the same IP Prefix is configured in more than one segment and the configuration is reverted by removing the IP Prefix from one of the segments, BfnFirewall agent restarts. (471757)
- IPv4 Multicast routes may be prematurely aged out (472845)
- If the system experiences a persistent configuration churn, an internal consistency check may cause a forwarding agent restart, which incurs a 100ms traffic outage. (474987)
- On the DCS 7170 series of switches using the stateless-load-balancer profile, if some of the servers in a nexthop-group are configured to be operationally down via CLI (server <ip> out-of-service) and health monitoring is disabled, other servers in the nexthop-group could also end up being marked operationally down. In the same way, if some of the servers are configured to be administratively down via CLI (server <ip> out-of-service graceful) and health monitoring is disabled, other servers in the nexthop-group could also end up being marked administratively down. Workaround is to remove the affected servers from the nexthop-group and add them back again. (483691)
- Hardware errors in the switching ASIC may get silently ignored after an initial reporting. (484277)

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

- Configuring more than five different speeds simultaneously on the system will result into continuous forwarding agent restarts. (339513)
Series Affected: 7300X3, CCS-720XP, DCS-7050CX3, DCS-7050SX3, DCS-7050X3, DCS-7260X and DCS-7260X3 Series

- When PTP is configured on a both a primary lane and a secondary lane on the same front panel interface, a speed change on the primary lane can cause an unexpected Strata agent restart, causing all lanes for that interface to become inactive until an ASIC reset is performed. This reset would result in all interfaces flapping. (390862)
- Graceful restart may not complete successfully for protocols configured on LAG interfaces during SSO. (460144)
Series Affected: DCS-7300X Series
- Egress queue will not get stuck even after the PFC storm is subsided in case of TCAM exhaustion during stuck event. (460915)
- Front panel 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. (475016)

SKUs Affected: DCS-7050TX3-48C8-F and DCS-7050TX3-48C8-R

DCS-7260X3 Series

- An internal power failure may cause a data plane outage requiring a manual reboot to recover (447040)
SKUs Affected: DCS-7260CX3-64-F, DCS-7260CX3-64-R, DCS-7260CX3-64E-F and DCS-7260CX3-64E-R

DCS-7050CX3, DCS-7050SX3 and DCS-7300 Series

- Performing SSU may lead to continuous traffic disruptions and/or certain features may not function correctly. (410242)

7368 Series

- show running-config incorrectly displays interfaces for non-inserted cards. Interface statuses for missing or powered down cards are displayed as inactive. (306105)
Series Affected: 7368 Series

CCS-720XP Series

- Speed changes cause a slow memory leak and an unexpected restart of the Strata forwarding plane agent. System is expected to recover and start normal operation following the restart. (441847)
Series Affected: CCS-720XP Series
- In multi-host authenticated mode, switch may send out untagged unicast identity requests to the tagged EAPOL supplicants which may cause them to not respond to the identity requests breaking their authentication. (447422)

- If a source interface is configured for radius in IPv6 scenario and "radius-server attribute 32 include-in-access-req" CLI is not configured, then neither NAS-IPv6-Address nor NAS-Identifier attribute gets sent in the RADIUS access requests. (459281)

vEOS Router Series

- Under limited circumstances, vEOS may experience issues with data plane traffic (471392)

BGP EVPN L2/L3 VXLAN/MPLS

- In EVPN VXLAN setup with IPv6 hosts when there are L2-only VTEPs publishing mac-only routes, Neighbor Solicitations from hosts behind a L3-VTEP for a target host behind a L2-only VTEP may be dropped without both proxy reply and flooding over VXLAN tunnel. This may happen only after the target host moves from the L3-VTEP to the L2-VTEP. The workaround is to apply a l2-vpn config on the L3-VTEP and add a deny proxy prefix list. (472048)

Known Software Caveats in 4.24.1

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)
- 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)
- The Macro-Segmentation Service (MSS) for Layer 3 firewalls may not correctly program traffic redirection/offload flows if the service is enabled prior to

DirectFlow being enabled on all switches.

A workaround is to shutdown the MSS service on CVX, enable DirectFlow on all supported switches and re-enable the MSS service. (366022)

Series Affected: DCS-7050, DCS-7050T, DCS-7050TX, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7250X, DCS-7260X, DCS-7260X3, DCS-7300 and DCS-7300X Series

- 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. (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)
- 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)
- Cspf agent may restart when TI-LFA is configured and the backup path is via a neighbor to which the point of local repair has ecmp paths and at least one path is not directly connected to the neighbor (427437)
- 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)
- When there're a lot of NAT translations synchronized through NAT Sync in a very short time period, NAT Sync may hang and stop synchronizing. Restarting Nat agent with "agent Nat terminate" in CLI Enable mode may help. Retrying the command several times may be needed. (467300)
- 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)
- In situations in which a large number of routes are forwarded over the same dynamic tunnel interface, the Arp agent may crash if the forwarding information of these routes are changed. The Arp agent will restart normally afterwards. (472837)
- At scale, some hardware BFD sessions may not be programmed. A workaround is to restart the Bfd agent. (473200)

- When adding a VRF during config replace or quickly deleting and re-adding a VRF, the internal state of the ARP agent may go out of sync and ARP entries may be missing from "show arp." Workaround is to delete the VRF and re-add it. (474469)

- NAT translations can't be synchronized through Nat Sync

A temporary workaround is to apply NAT profiles on both peers in strictly the same order starting from a clean config with no NAT-related config included, and config those to-be-sync'ed NAT profiles first. (478219)

- 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)
- Entering IPv6 addresses in the VxLAN flood list result in removal of previously configured IPv4 addresses, resulting in impact to forwarding behavior. As a workaround, do not configure IPv6 addresses as part of the floodlist. (490613)

Multi-agent

- Performing a stateful swtichover 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)
- The Bgp agent may restart unexpectedly if auto-local-addr is configured on a neighbor that is in the process of being established. (433805)

- When a disconnected RPKI cache changes to non-preferred due to a change in cache preferences, the Rpkid agent will stop attempting to reestablish the TCP connection to the cache. It will remain in this state even after the disconnected cache becomes the preferred cache again. Running "clear bgp rpkid cache <cache name>" will cause the Rpkid agent to resume attempting to reestablish the TCP connection. (464719)
- When a large number of updates are backed up in the transmit socket buffers, it may sometimes lead to the BGP neighbors session getting stuck in Idle (PendingNotification) state when the session reset is attempted and BGP is unable to send a notification. Not being able to send out updates may lead to traffic misforwarding or drops. (466575)
- Bgp agent restart may be not be hitless, even if Graceful Restart is configured, due to connection collision resolution closing the wrong connection.
A workaround is to configure one of the peers as passive, so that it waits for the remote peer to initiate the connection, avoiding connection collisions entirely. (468036)
- Sometimes BGP (multi-agent) would advertise an incorrect originator-ID when sending updates to iBGP clients when configured as route-reflector. The problem only manifests when different paths (could be paths belonging to the same prefix or different prefixes) have the exact same path attributes, including NextHop. The problem corrects itself if the paths are resent to the route-reflector from the source whose paths had the incorrect originatorId. This problem can manifest with add-path configuration as well when the additional paths have the same path attributes. (472025)
- During a hitless restart of the Bgp agent, 'update wait-for-convergence' behavior is unnecessarily forced for AFI-SAFIs which do not support hitless Bgp agent restart. (475840)
- 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)
- During SSU or SSO, 'update wait-for-convergence' behavior is unnecessarily forced for AFI-SAFIs which do not support SSU or SSO. (483591)
- RCF functions relying on prefix comparison may return incorrect function evaluation results. (484550)
- UCMP is not supported for FECs pointed to by routes in a VRF which are the result of reachability information learnt outside of BGP IPv4 and IPv6 unicast address-family (e.g: L3 EVPN, L3 MPLS VPN, BGP-LU, 6PE, etc)

If UCMP is enabled for BGP in such cases, the IpRib agent may restart

continuously when processing FECs for such other address-family routes.
(487511)

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)

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 a SSO switchover 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)

- In VXLAN deployment, remapping the VNI from one VLAN to another VLAN may cause the destination VTEP to drop ARP requests received over VXLAN tunnel in that VNI. (482403)
- "%SPANTREE-4-BLOCK_RATELIMITER: Exceeded BPDU rate limiter on <INTF>" may be logged and INTF errdisabled if spanning-tree mode is not rapid-pvst or "spanning-tree mst pvst border" is not configured and sflow is configured on the switch in a network where PVST is enabled on other switches.

To work around, disable sflow on the affected interface. (487260)

Layer 1

- Speed change on interfaces with "speed-misconfigured" errdisable state after hitless reload causes forwarding agent restart. This leads to the flap of all connected interfaces. The workaround is to recover all "speed-misconfigured" interfaces by configuring speeds of affected /2, /3 and /4 ports to match the speed of the corresponding /1 ports before hitless reload. (352115)
Series Affected: DCS-7060X and DCS-7060X2 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
- 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)

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)
- Maintenance enter operation may be stuck for System unit on an MLAG switch after upgrading from an older release and Mlag agent may restart unexpectedly while exiting maintenance mode. To workaround, create a user-configured unit with all the BGP and interface groups of System unit and use the user-configured unit for maintenance operations instead of System unit. (483610)

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)
- SSU with Splunk enabled may result in extended boot times, which could lead to protocol timeouts or switch cold rebooting. (343629)
- When running 'reload fast-boot' or 'reload hitless', ports with optical transceivers may flap, causing traffic disruption (348172)
 SKUs Affected: DCS-7050SX-128-F, DCS-7050SX-128-R, DCS-7050SX-128-SSD-F, DCS-7050SX-128-SSD-R, DCS-7050SX2-128-F, DCS-7050SX2-128-R, DCS-7050TX-48-F, DCS-7050TX-48-R, DCS-7050TX-64-F, DCS-7050TX-64-R, DCS-7050TX-72Q-F and DCS-7050TX-72Q-R
- 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

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)
- MSS revokes redirect rules from a MLAG peer when the last member interface on any of the port channels connected to the service device goes down. This results in redirected traffic traversing that MLAG peer being dropped.

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. (230653)

- 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)
- If there are large number of intercept hosts in L2 policies in the order of 10k, then shutting down management cvx feature may not cleanup all DirectFlow rules (285821)

- The Macro-Segmentation Service (MSS) interfacing with a firewall running in L2 transparent mode does not enforce a firewall policy that requires intercepting traffic on a VNI for the first time while one of the peers of the MLAG Service VTEP is being reloaded. MSS starts intercepting that set of hosts when the peer reload completes. (373587)
- 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)
- In Macro-Segmentation Service (MSS) configuration, the firewall credentials are displayed without encryption in MssPolicyMonitor agent log files. This happens for any firewall currently supported. (470768)
- When CVX receives a malformed control-plane message, the ControllerOob agent may restart. This can trigger HA failover of the CVX cluster. (483850)
- OpenStack dynamic VLAN to VNI mappings for OpenStack Ironic baremetal hosts will be removed from CVX client switches if the VirtualNetwork agent is restarted (486304)

MPLS

- Arp agent may crash continuously in cEOS-lab container when a static MPLS route pointing to a nexthop-group is configured. (477494)

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)

- When routing is disabled, ARP control packets share the CPU queue with other CPU bound packets. This could lead to MLAG disassociation and network outages.

The workaround is to either enable IP routing or have a static ARP entry on the MLAG peers. (90138)

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

- Enabling the Macro-segmentation service can result in duplicate packet delivery of broadcast, multicast or unknown unicast traffic sourced from the host whose traffic is intercepted. Additionally, one copy can be delivered to the intercepted host that is the source of the traffic. (212480)
- 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 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)
- OpenConfig affected by CVE-2019-6486 (356552)
- 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-7280E, DCS-7280R, DCS-7280R2, DCS-7500E, DCS-7500R and DCS-7500R2 Series

- Nitrogen ODL gives an error reading the path /interfaces/interface/arista-vxlan (370169)
- 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)
- Mlag agent may crash if the system is being put in Maintenance Mode if interface profile has shutdown max-delay enabled. Workaround is as follows:
 1. Create a maintenance interface profile which does not have shutdown max-delay configured with profile name being lexicographically largest.

```
profile interface zzz_no_shutdown_delay
  rate-monitoring threshold 4294967295
```

2. Create an interface group constituting all the physical ethernet interfaces of peer-link and attach the above interface profile that does not have shutdown max-delay configured.
 3. Create a unit with this group and quiesce it. (380387)
- 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 may restart unexpectedly. (407002)
 - If the number of PTP vlan's enabled on a switch using 'ptp vlan' command exceeds 65536, PTP agent will become unresponsive 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)
 - Configuring IPv4-mapped IPv6 Address in an ACL leaves OpenConfig in an inconsistent state preventing any further OpenConfig Update operation. (471220)
 - 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-7280E, DCS-7280R, DCS-7280R2, DCS-7280SE, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500E, DCS-7500R and DCS-7500R2 Series
- If FIB optimization configuration is present in startup config, it is accepted on platforms that do not support the feature leading to incorrect routes being programmed in the hardware. This causes incorrect routing. To workaround this problem, remove the optimization configuration from the startup config and reload the switch. (478338)
- In an EVPN deployment, ARP entries maybe not be cleared when it's Type 2 route is withdrawn. (478941)
- On systems with many update notifications from eos-native paths, the Octa agent log files could fill up with spurious errors. (482039)
- Octa sends more data than requested for a gNMI Subscription with origin "eos_native" and mode SAMPLE. (482142)
- Octa may restart unexpectedly when handling a gNMI Subscription with origin "eos_native" and mode SAMPLE. (482143)

Multicast

- 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)
- In an environment with a very large number of MSDP peers, during cleanup the Msdp Agent may crash. (354364)
- 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-learned 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 crash. (418190)

- When static multicast routes are configured, in some cases the IgmpHostProxy agent may not create reports for all of the mroutes. As a workaround, after this occurs, deleting and recreating the static mroute should fix the IgmpHostProxy agent state. (449133)
- Hosts attached to a VLAN could see a increased delay in receiving the initial multicast stream at times when the host sends reports at certain low latencies. (475942)
- High CPU utilization might be observed for the forwarding agent when PIM Bidir routes are present. (479119)
- When using Sfe based forwarding configuration, the BessMgr agent may restart unexpectedly when multicast packet size is greater than 1500 bytes (481192)
- 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

DCS-7150 Series

- If a multicast boundary is applied on an SVI which also has IGMP snooping enabled, IGMP snooping will not take effect. (138610)

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

- 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)

- When a sub interface under lag member configured with shaping is removed, IP ACLS stops working on port-channel sub-interfaces. (162785)
- 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)
- 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)
- 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-7500E and 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 to 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)
- 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)

- In the presence of virtual MAC with mask configuration, packets that undergo recirculation may not be properly forwarded. The workaround is to eliminate the configuration that causes the recirculation to happen. (387535)
- If VXLAN is configured, PBR and QOS policies won't apply to traffic ingressing on a MLAG peer-link. (390804)
- Traffic subject to CPU traffic policy `_policer_` action will not be `_forwarded_`. This includes multicast control traffic which is replicated to both the CPU but also forwarded (e.g. PIM, OSPF HELLOs, etc.). Unroutable unicast traffic is also flooded, and so will not be forwarded if matched by a CPU traffic policy policer action. An example policy of concern is

```
traffic-policies
  traffic-policy EXAMPLE
    match PIM ipv4
      protocol pim
      actions
        police rate 1024 kbps
```

In this example, PIM control packets would be policed to 1024 kbps to the kernel, but dropped completely on any outbound interface.

NOTE: If the traffic subject to policing is only bound for the CPU port (e.g. unicast control plane traffic such as BGP packets), there is no impact. (395561)

- 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)

- Insertion of a fabric module may cause brief traffic loss on the device (402508)
SKUs Affected: 7504R3-FM and 7508R3-FM
- When configure replace is used to configure large acl configurations, the configuration might time out and the new configuration may not apply. The workaround is to make smaller changes in the acl configuration. (404797)
- TCAM reservations are not preserved after a system reboot. (410069)

- With multiple configuration operations, such as add/modify/delete, on QoS policy maps, a restart of SandAcl agent may result into a core file and hitful operations for a brief period when 'feature qos mac' is in use. (410390)
- 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)
- 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)
- If an egress-ip6-acl is applied on a shut SubIntf and then the SubIntf is unshut then Default-deny rule of the egress-ipv6-acl doesn't work. Reapplication of the acl resolves the issue. (445371)
- 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)
- Increased TCAM usage after reload if startup configuration has Acls for Ingress Ipv4 security Acls, QOS, PBR, FlowSpec, CPU Traffic Policy, and TapAgg when configured on SVIs. The increased TCAM usage may result in some ACLs not getting programmed in hardware. (451463)
- 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 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)
- Pre existing DirectFlow flows may temporarily fail to be effective while new flows are being installed. (460230)
- EventMgr Agent may crash after a manual linecard hotswap. A temporary workaround is made to disable the following functionalities:
 - VOQ Delete event management
 - Environment related health metrics like 'cooling', 'power', 'voltage' and 'temperature' under 'monitor device-health' configuration mode (464788)
- 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)
- Configuring `port qualifier size <number-of-bits> bits` on `feature flow-spec port ipv4` but not in `feature flow-spec port ipv6`, or vice versa may cause the SandAcl agent to restart continuously.

To recover, configure the `port qualifier size` on both features with the same size. (476298)

- If the number of BGP Flowspec matches exceed the hardware TCAM banks and entries available, and then Flowspec is enabled on additional interfaces while in the overflow state, the matches may fail to be programmed on the additional interfaces, even if the published Flowspec matches later fall back under the hardware limits. (477150)
- 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)

- 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)
- The 'fragment offset' match field is not supported on CPU Traffic Policies. When a CPU policy containing 'fragment offset' match criteria is applied, SandAcl will crash repeatedly. (479689)
- Restarting the SandAcl agent while BGP Flowspec is applied on more than the supported number of VRFs can lead to unexpected traffic behavior. (481575)
- Packet egressing on an L2 SubInterface might egress untagged when the TC-to-COS profile applied on it is altered. The workaround is to do shut followed by unshut of the concerned SubInterface. (481745)
Series Affected: DCS-7020, DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series
- When link-down debounce is configured, if at the expiration of the debounce timer the PCS is link up but local fault is present, remote fault will not be sent to the peer if the link remains down past the link-down debounce period, resulting in a unidirectional link.

The workaround is to not configure link-down debounce. (482636)

Series Affected: 7300X3, 7320X, 7368, DCS-7160 and DCS-7170 Series

- When subinterface connectors using in patch panel and subinterface dot1q encapsulation has both outer/inner tags, packets forwarded to the Tx port corresponding to subinterface will have incorrect tags. An extra tag with VID=0 is inserted. (485071)
- 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)

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)
- In an EVPN MPLS configuration, broadcast ARP requests may not be forwarded when the TCAM profile doesn't have the feature 'evpn mpls irb'. The workaround is to add the feature 'evpn mpls irb' to the TCAM profile. (487198)
- With mpls-evpn system profile, post mpls termination ip routes may not work with "ip hardware fib optimize prefixes profile internet" configuration. (489268)

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)

DCS-7020RA, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards Series

- VXLAN packets that are decapped and bridged are incorrectly subject to the IP ACL applied on the ingress port. (221457)
- When AlgoMatch is enabled, packets may be unexpectedly dropped if ACLs are applied and an interface has a double tag VLAN mapping. (229765)
- The HaloFpga agent will continuously restart if SandFap agent is restarted.

The workaround is to powercycle the linecard or powercycle the switch if it's a fixed system. (252069)

- 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)

DCS-7280R3 and DCS-7500R3 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)
- Configuring "hardware access-list qos resource sharing routedport subinterface" will cause traffic ingressing on a subinterface to match a policy-map configured on a front-panel port. Routed ports and subinterfaces sharing TCAM entries is not supported on this platform and the command should not be used. (470778)
- 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)
- When a QoS policy-map is configured on an SVI and a subinterface on the same core it may result in traffic rates from those interfaces to be policed as one.
Configure separate QoS policy-maps on SVI and subinterfaces on the same core to ensure the policer working as per configured rate. (484274)
- Outer DSCP is not derived from Traffic Class in VXLAN encapsulated bridged packet. (487274)

DCS-7280E and DCS-7500E Series

- On the DCS-7280E and DCS-7500E series, disabling autonegotiation on a port with a 1G fiber transceiver can cause occasional link flaps.

The workaround is to always enable autonegotiation on these ports. (70667)

- IPv4 egress RACLs will not filter multicast traffic in shared mode. In unshared mode, multicast traffic is filtered only if ingress replication is enabled. (131660)
- An IPv6 Egress ACL applied to a Port Channel is not applied to a newly added member interface, if the member interface already has the same ACL applied to it. The workaround is to remove the ACL from the interface before adding it to the PortChannel. (141736)
- SAND_POSSIBLE_STUCK_PORT may be logged on an Ethernet interface after switch initialization, which can cause an interface to not transmit packets despite being up.

A workaround is to perform a full reset of the corresponding forwarding chip using the "reset platform arad <forwarding chip name> full" command. All Ethernet interfaces on that forwarding chip will flap; to determine all the Ethernet interfaces on the forwarding chip, run "show platform arad <forwarding chip name> map | grep Ethernet". (201096)

- In multi-agent mode, configuring multiple VRFs and Vxlan routing may lead to continuous OOM failures. (399674)

DCS-7160 Series

- Under certain race conditions between LAG configuration changes and XpCentral agent restart, the system could get into a state where XpCentral agent continuously undergoes a restart.

The workaround is to remove all LAG interfaces and re-configure them after XpCentral agent has restarted successfully. (161558)

- When mirroring destination is configured to CPU, under heavy traffic scenarios, it may be possible that switch engine ASIC may leak some packet buffers, and may eventually run out of them causing switching to stop forwarding packets on one or more ports.

Workaround is to not configure mirroring destination as CPU for a prolonged duration under sustained linerate traffic. (225142)

- 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 crash 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

DCS-7170 Series

- If a LAG was created with member-ports in shutdown state, outgoing traffic can incorrectly get hashed to those member links leading to traffic loss. (250543)
- On the 7170, when dynamic NAT is configured on the layer 3 interfaces used for ECMP, return traffic does not get NAT applied unless it comes in on the same ECMP member of the outbound NATted traffic. (398104)

Series Affected: DCS-7170 Series

DCS-7170 Series

- If a mac learnt on a vxlan interface on an MLAG peer is promoted due to an event such as a MLAG peer-link going down, it may cause the forwarding plane agents to restart. (261152)

7368X, CCS-720XP, DCS-7010, DCS-7050X, DCS-7060X, DCS-7250X, DCS-7260X and DCS-7300 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-7050 and DCS-7050X Series
- The WRED drop decision obtained from the ECN configuration on tx-queue 0 is also used to determine whether packets should be dropped on UC8. This can result in control packets enqueued on UC8 getting dropped if UC0 is experiencing WRED drops for non ECT packets enqueued on it. A workaround is to use a queue other than tx-queue 0 for applying ECN. (125803)
Series Affected: DCS-7050 Series
- MAC ACLs and PACLs cannot co-exist on the same interface if QoS policy ACLs exist in the switch (186949)
- On an MLAG pair of switches, with fast-MAC redirect enabled, the Macro-Segmentation Service (MSS) can fail to recover from a MLAG port channel member link flap.

The workaround is to shut/ no-shut the port channel connected to the intercepted host experiencing traffic loss. (213199)

Series Affected: DCS-7050X and DCS-7060X 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: DCS-7010, DCS-7050, DCS-7050T, DCS-7050TX, DCS-7050X,

DCS-7050X2, DCS-7050X3, DCS-7060X, DCS-7060X2, DCS-7260X, DCS-7260X3, DCS-7300, DCS-7300X and DCS-7320 Series

- If nexthop resources are exhausted as indicated by syslog `VXLAN_HWHER_NEXTHOP_RESOURCE_FULLL`, 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-7300 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)

- 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)

- In ALPM mode, If TCAM is unable to accommodate route with prefix < 64 but is able to accomodate prefix > 64, in that case StrataL3 might crash during route addition or deletion. (282009)
- If SSO redundancy mode is configured and a linecard is removed before it is fully initialized, RPR switchover may be performed. (283088)
Series Affected: DCS-7300X Series
- 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

- 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

- 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-7300 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)

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

- After lowering the priority of a flow, traffic may continue to match on that flow even if existing flows now have higher priority. Updating flows priority again or toggling DirectFlow should restore expected behavior. (408312)

- 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

- For pfc enabled ports across multiple line cards, a congestion on the egress side is not producing any tx back pressure from the ingress side. (409148)

- 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, DCS-7300, DCS-7300X and DCS-7320 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)

- 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)
- On ECMP shrinkage due to link down events, VXLAN tunnels reachable via ECMP may experience extended outage until routes reconverge. (419753)
- 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

- 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 an ASU upgrade, interfaces with 100GBASE-SRBD transceivers may experience a single link flap. (440451)

Series Affected: DCS-7260CX3 Series

- 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)
- When STRATA-4-HW_PORT_RESOURCE_FULL log appears in syslog, some 25G interfaces might discard all received packets. In the output of "show interfaces status" command, QSFP100 interfaces might be affected if any of the /2-4 interfaces is inactive when the QSFP100 port is configured to do 4x25G. (464667)
 SKUs Affected: DCS-7050SX3-48YC8-F, DCS-7050SX3-48YC8-R, DCS-7050TX3-48C8-F and DCS-7050TX3-48C8-R
- 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)
- Changing the speed of a subordinate port will cause the rest of the ports on a QSFP port to flap. (472767)
- VXLAN remote MAC entries may not be properly recovered in some cases across ASU and SSO resulting in flooding for those macs. (477643)
- 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)
- With PFC pause stream for lossless priorities on egress interface and data traffic destined to the egress interface for lossy and lossless priorities, indefinite traffic loss may be seen on lossy priority traffic on toggling PFC globally.
 Workaround - Stopping PFC pause frames, Strata slice agent restart, Enabling watchdog on PFC received interface. (477954)
 SKUs Affected: CCS-720XP-24Y6-F, CCS-720XP-24Y6-R, CCS-720XP-24ZY4-F, CCS-720XP-48Y6-F, CCS-720XP-48Y6-R, CCS-720XP-96ZC2-F, DCS-7050CX3M-32S-F, DCS-7050CX3M-32S-R, DCS-7050SX3-48YC12-F, DCS-7050SX3-48YC8-F, DCS-7050SX3-48YC8-R, DCS-7050SX3-96YC8-F, DCS-7050SX3-96YC8-R, DCS-7050TX3-48C8-F and DCS-7050TX3-48C8-R
- Updating an already installed QoS policy-map might result in certain rules of the policy-map not taking effect in hardware.

A workaround is to remove this QoS policy-map from all the interfaces where it is applied first and then reapply it on all the desired interfaces. (478549)

- 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
- When PIM is enabled on one or more VxLAN VLANs, disabling the 'vxlan1' interface (using the 'shut' CLI command) may cause multicast data traffic ingressing on these VLANs to get looped or blackholed.
 Removing the VNI mapping configuration for these VxLAN VLANs will restore normal traffic forwarding. (483646)
 Series Affected: DCS-7050TX, DCS-7060CX, DCS-7060CX2, DCS-7060SX2, DCS-7060X and DCS-7060X2 Series
- Egress mirroring to CPU may not function correctly. Egress mirroring to CPU may be configured but packets will not be sent to CPU. There is no workaround for this. (484079)
 Series Affected: 7320X, DCS-7250X, DCS-7260CX and DCS-7300X Series
- Aggregate storm control rate limit is not honored for broadcast and multicast traffic. (490511)

DCS-7050X2 and DCS-7300 Series

- When an interface which is transmitting at line rate 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)
- If the switch receives a VLAN-tagged VXLAN encapsulated packet destined to the switch's VTEP IP address, but the packet's destination MAC is not the switch's MAC, such a packet is flooded to all ports in the ingress VLAN including the ingress physical port. (261494)

DCS-7010T Series

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

DCS-7060X and DCS-7300 Series

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

DCS-7050 and DCS-7300 Series

- 25G optics are not supported. Inserting one would lead the forwarding agent to crash continuously. (199036)

DCS-7260X3 Series

- Ports with 1g transceivers will still count towards the limit of 5 speed classes even when disabled and may lead to continuous restart of the Strata forwarding agent. It can cause traffic outage on other ports.

Workaround is to remove the 1g transceiver. (338741)

- 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)

DCS-7050CX3, DCS-7050SX3 and DCS-7300 Series

- Egress ACL on SVI for BUM traffic will not match ACL rules for packets being sent across fabric interfaces. (284543)
- When performing SSU, there may be failure in table programming resulting in fatal error cold reboot with extended traffic outage. (399774)
- 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)
- 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)
- When the uRPF feature is disabled and enabled in quick succession, the switch may enter an inconsistent state and may stop routing traffic. Workaround is to repeat the same steps with an interval of about 5 seconds between the two operations. (480331)
- "platform trident unknown-mac-drop" command is not honored for packets that are routed and flooded on the egress VLAN. There is no workaround for this. (481755)
- 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-7300 Series
- Aggregate storm control rate limit is not honored for traffic that is routed and flooded in the egress VLAN. (485492)

7368 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)

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 resolve the issue. (368424)
- PTP timestamps may occasionally jump 4 seconds back in time. The switch will recover on its own after a few minutes of synchronizing with the PTP grandmaster again. (490501)

DCS-7050X and DCS-7300 Series

- Layer 1 related configuration changes (e.g. speed, shutdown, no shutdown) can cause the forwarding slice agent to crash, causing all the ports to flap. (110720)
SKUs Affected: DCS-7050SX-128-F, DCS-7050SX-128-R, DCS-7050SX-128-SSD-F and DCS-7050SX-128-SSD-R
- 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)
- 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)

DCS-7300 and DCS-7500 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 crash repeatedly in rare corner case and Management0 interface is not reachable in Modular systems. Doing switchover will address the issue. (369565)
- After a stateful switchover, EOS may not monitor chassis power failures. This may result in cards staying powered off even if the chassis power recovers. (486749)
SKUs Affected: DCS-7516-SUP2 and DCS-7516-SUP2-D
- All fabrics and linecards may power down upon removal of the active supervisor (490109)
SKUs Affected: DCS-7516-SUP2 and DCS-7516-SUP2-D

DCS-7020RA, DCS-7160, DCS-7170, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards 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 Halo 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 continuously crash. A reboot or linecard reset is required to clear this condition. (486369)

Series Affected: DCS-7280R2 and DCS-7500R2 Series

Containerized EOS Series

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

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)

vEOS Router Series

- The OpenFlow agent fails to handle packet-in messages (145001)
- 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)
- 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)

BGP EVPN L2/L3 VXLAN/MPLS

- DF election may not work correctly after changing VLAN - VNI binding. (484811)

Limitations and Restrictions in 4.24.1

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)
- BMP is not supported for router bgp instances configured in non-default VRFs. (210363)
- 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)
- The command "[no] service routing configuration route-map no-set-community explicit-members"

affects the behaviour of the route-map command

"no set community [community-list] [member]+ [action]".

If "service routing configuration route-map no-set-community explicit-members" is enabled, only "set community" statements in the routemap that are referred to by the list of members in the "no set community" command will be affected. The default behavior is to remove all "set community community-list" commands from the routemap. (330839)

- 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-7050, DCS-7050T, 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)
- When MPLS tunnel egress counters or next-hop group counters are enabled, forwarding plane agent restarts could see traffic loss (435899)

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 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)

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)

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)
- Negation operator (!) and 'assigned' keyword are not supported in Radius NAS-Filter-rule(attribute-id 92) Attribute. (475207)

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-F, DCS-7280SRAM-48C6-R, DCS-7280SRM-40CX2-F and DCS-7280SRM-40CX2-R

MLAG

- Spanning-tree mode backup does not work in an MLAG configuration. (15151)
- 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)

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-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)

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)

- 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)
- Mss does not support traffic interception for the hosts connected to Service VTEP. (354754)
- 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)
- 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 Pol is the MLAG peer link):

```
flow bypassPeerLink
    priority 65535
    table trident ifp
    match input interface Pol
    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 Pol103    >>>>>>> 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)
```

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)

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)
- Private VLAN is not supported in the EOS image distributed to US customers. (159408)
- 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)

- Enabling next-hop sharing (using "ip hardware fib next-hop sharing" command) could result in slower convergence in the case of link failures. (369305)
- 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 IP Locking 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 may cause the Aaa agent to continuously restart (439333)
- 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)
- Currently EOS does not support parsing and separating multiple ACL rules in the same NAS-Filter-Rule AVP using zero byte delimiter. (475210)
- EOS Extension Manager does not allow installing a 64-bit rpm as an extension if the 32-bit rpm of the same name is already installed (and vice versa). This is because of a missing rpm architecture check. For example, 32-bit EOS will not allow install of 64-bit glibc rpm as an extension claiming that rpm is already installed. (487943)

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 crash 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)

DCS-7150 Series

- Under extreme circumstances where a high volume of broadcast or multicast traffic is sent from 10G ports to a mix of multiple 1G ports and one or more 10G ports, continuous over-subscription of the 1G interfaces could result in consumption of all system queue descriptors.

If this occurs, the 10G ports may be limited to 1G transmission rates. While this is an extreme case, CLI commands can be used to tune the maximum queue length available to 1G interfaces to mitigate this risk. (32294)

- NAT translation does not happen for a packet if the ARP for the next-hop is not resolved or is aged out. Translation will start happening again once ARP resolution completes.

The workaround is to install a static ARP entry for the next-hop that the NAT translated packet will take. (40132)

- Source port loopback suppression at high traffic rate can reduce the egress bandwidth of a port. This will happen when a port forwards incoming multicast traffic at a high rate to a multicast group which also has this port as a member. This port will receive back copies of the replicated

traffic and drop them due to loopback suppression if there are no receivers on it at the egress stage of the port. (40294)

- NAT and VXLAN cannot be configured on the switch at the same time. (47258)
- When agile ports are configured for 40G with clause 73 autoneg (speed auto 40gfull) while using CR cables, the ports cannot be used in a port channel.

The workaround is to force the speed to '40gfull' on the ports. (55517)

- Systems with A0 silicon, packets are not forwarded to the egress port when egress truncation and timestamping are enabled together. Removing the configurations resumes packet forwarding. Truncation and timestamping are not supported together. (72756)
- The VXLAN flood VTEP list cannot be more than 128k VLAN-VTEPs, where VLAN-VTEPs is the number of VLANs multiplied by the number of VTEPs. (73228)
- Ingress port access control list (PACL) on a VXLAN-enabled interface is not supported. If ingress PACL is configured on a VXLAN-enabled interface, in-hardware VXLAN encapsulation of incoming packets is not expected to work correctly. VXLAN encapsulation of packets in software is not affected. Removing ingress PACL configuration on the affected interface restores correct VXLAN hardware encapsulation behavior on that interface. (76085)
- Multicast-routed frames get tx-mirrored even when they do not egress the tx-mirrored multicast destination due to VLAN suppression. This is a limitation of the switch ASIC. (87933)
- Enabling counters for Static or Twice NAT connection can cause FocalPointV2 agent restarts, when the number of connections exceed 275. (109048)
- On a DCS-7150 series switch, VXLAN encapsulating a packet post routing may result in the outgoing packet being corrupted if the packet was permitted by an ACL with "statistics per-entry" enabled. (294588)
- IPV6 hop-limit based filter in access-list is not supported even if accepted by CLI. (383400)

Series Affected: DCS-7150 Series

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

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

- Linecards with HW revision < 02.00, when configured for 100G and a physical layer problem is present, a one-way link may result. The link experiencing the physical layer problem will be down. However, the peer link may still be up.

The workaround is to detect this situation, by, for example, looking at the link status on both sides of the 100G link, and perform remedial actions; for example, replacing the transceiver or cable. Running a keepalive protocol like LACP on these links is advised. (67325)

- show interfaces counters rates' for port channels may show a slightly inaccurate data rate (including above 100%). (67367)
- Linecards with HW revision < 02.00, under extreme scenarios where we receive linerate small packets on all interfaces connected to the same forwarding ASIC and ingress mirror or sflow dangerous is turned on many of these interfaces, some packets (both the original and the mirror/sFlow copy) can be dropped. (67942)
- 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)
Series Affected: DCS-7500E Series
- 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 running PTP with 4X10G break-out cables, a variable delay is observed with the PTP timestamps that can cause instability to the PTP time calculations. (186891)
- 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)
- Linecards with HW revision < 02.00, IP-in-IP encapsulated packets might not get forwarded after termination if the packet size falls within the range 223-287 bytes. (193573)

- 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)
- On devices with Algomatch enabled, decapsulation of an outer IPv6 header will not work. (215833)
- 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-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)
- After applying or removing shaping configuration on an L2 subinterface, the L2 subinterface must be flapped for the configuration to take effect. (278730)
- 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)
- With uRPF configuration, packets sent by the Cpu that match a route forwarding into MPLS, GRE, or a Vxlan tunnel are incorrectly dropped in the hardware due to uRPF violation. (343891)
- Stale telemetry flow-spec statistics may be seen until the next "show flow-spec" command is issued. (345195)
- Enabling Route Exact Match may cause security ACLs (Port ACLs, Router ACLs & MAC ACLs) to stop working when AlgoMatch hardware is also enabled. (348149)
- Filtered mirroring is not supported on linecards or fixed-systems operating in TAP Aggregation mode when traffic steering is enabled. (349883)
- 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)
- 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)

- Different streams being rate-limited by the same policer might exhibit bias towards some streams and fair policing across all the streams is not guaranteed. (380599)
- 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% line rate (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 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-7280E, DCS-7280R, DCS-7280R2, DCS-7280SE, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500E, DCS-7500R and DCS-7500R2 Series

DCS-7280R and DCS-7500R Series

- An IPv6 MPLS 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)
- If mirroring to CPU is configured for an interface and an incoming MPLS packet on that interface matches a configured "mpls static vrf-label" entry, the packet will not be mirrored to CPU. (359362)
- 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-7048, DCS-7280CR2, DCS-7280E, DCS-7280R, DCS-7280R2, DCS-7280SE, DCS-7280SR, DCS-7280SR2, DCS-7280TR, DCS-7500E, 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

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
- The current implementation of IPSec supports only encryption/authentication algorithm combinations of AES128/SHA1 or AES256/SHA256. No other combinations are currently supported. (359986)
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-7280R3 and DCS-7500R3 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)

- Traffic drop may happen when we sent traffic to all 8 traffic-classes (aggregate rate nearing line rate) to port which has been configured with Strict-Priority scheduling. (406550)
- Traffic drop may happen when we sent traffic to all 8 traffic-classes (aggregate rate nearing line rate) 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)
- Set dscp 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)
- 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)
- VPWS steering through SRTE along with control word configuration is unsupported. Remove control word from VPWS configuration otherwise the SandL3Unicast agent may restart repeatedly. (490325)

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 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)
- ACLs with Vxlan is not supported, and may result in unexpected forwarding behavior depending on the configuration and pipeline profile. (217888)
- 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 mililiseconds of packet loss when VxLAN ECMP nexthop changes. (219888)
- There may be traffic loss of up to 100 mililiseconds 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)

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
- BFD sessions are not supported on Port-channel interfaces. The sessions will not come up. (250315)
- 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)
- 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)

7368X, CCS-720XP, DCS-7010, DCS-7050X, DCS-7060X, DCS-7250X, DCS-7260X and DCS-7300 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)
- L3 packets destined to a next hop whose MAC address is not learned and which fail the uRPF check configured on the incoming SVI are flooded in the ingress VLAN. (75660)

Series Affected: DCS-7050 Series

- 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)
- 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)
- 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-7300 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)
- 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)
- 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)
- 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-7010, DCS-7050, DCS-7050CX3, DCS-7050Q, DCS-7050S, DCS-7050SX2, DCS-7050SX3, DCS-7050T, DCS-7050TX, DCS-7050X, DCS-7050X2, DCS-7050X3, DCS-7060CX, DCS-7060CX2, DCS-7060SX2, DCS-7060X, DCS-7060X2, DCS-7060X3, DCS-7060X4, DCS-7250X, DCS-7260CX, DCS-7260CX3, DCS-7260QX, DCS-7260X, DCS-7260X3, DCS-7300, DCS-7300X and DCS-7320 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-7050CX3, DCS-7050SX3, DCS-7050X3, DCS-7060X3, 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: CCS-720XP, DCS-7050CX3, DCS-7050SX3, DCS-7060X3, DCS-7060X4 and DCS-7300X 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)
- 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)

DCS-7050X2 and DCS-7300 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)
- 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)

DCS-7010T Series

- IEEE 1588 PTP transparent clock does not decrement TTL for PTP routed packets (55078)

DCS-7060X and DCS-7300 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

- LANA is not supported. (217543)
- Configuring 100G, 50G, 40G, 25G and 10G simultaneously might result in unexpected packet forwarding behavior. (235075)

DCS-7050CX3, DCS-7050SX3 and DCS-7300 Series

- 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 and 7300X3-48YC4-LC
- 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
- 50g port speed is not supported in this release (445999)
SKUs Affected: DCS-7050CX3M-32S-F and DCS-7050CX3M-32S-R

7368 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)

CCS-720XP Series

- When hardware or software flow tracking is enabled, Vxlan encapsulated TCP flows may get exported with incorrect tcpFlags. The tcpFlags field track outer header's TCP flags hence for Vxlan packets it is undefined. There is no workaround to this issue. (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)
- 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)

DCS-7050X and DCS-7300 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)
- EOS will fail to detect modules, such as some 100GBASE-DWDM4 modules, that require deassertion Low Power Mode (LPMODE) pin to be de-asserted. (160016)
Series Affected: DCS-7050S and DCS-7050T Series
- 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 unlearned. 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)

DCS-7300 and DCS-7500 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)

DCS-7020RA, DCS-7160, DCS-7170, DCS-7280R2A, DCS-7280RA and DCS-7500R with 7500RA or 7500R2A linecards 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)

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)

vEOS Router Series

- 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 deattching 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 Telemetry control packets (default UDP destination port is 4789) with a higher priority. (434087)

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)

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.