Arista Networks EOS 4.18.5M Release Notes

Version: 1.1

17 November 2017

Table of Contents

EOS 4.18.5M Release Highlights

New Platforms and Hardware

- None

SNMP MIBs

- SNMPv2, SNMPv3
- RFC 3635 EtherLike-MIB
    - obsoletes RFCs 1650, 2358, 2665
- RFC 3418 SNMPv2-MIB
    - obsoletes RFCs 1450, 1907
- RFC 2863 IF-MIB
    - obsoletes RFCs 1229, 1573, 2233
- RFC 2864 IF-INVERTED-STACK-MIB
- RFC 2096 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 2013 UDP-MIB
    - obsoletes RFC 1213
- RFC 2012 TCP-MIB
    - obsoletes RFC 1213
- RFC 2011 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-BGPV4V2-MIB
- ARISTA-VRF-MIB
- ARISTA-DAEMON-MIB
- ARISTA-ECN-COUNTER-MIB
    - 7500R, 7500E, 7280R, 7280E
- 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

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, vrrpTrapAuthFailure

Supported Hardware

Fixed System

- DCS-7010T-48
- DCS-7010T-48-DC
- DCS-7050Q-16-F
- DCS-7050Q-16-R
- DCS-7050S-52-F
- DCS-7050S-52-R
- DCS-7050S-52-SSD-F
- DCS-7050S-52-SSD-R
- DCS-7050S-64-F
- DCS-7050S-64-R
- DCS-7050S-64-SSD-F
- DCS-7050S-64-SSD-R
- DCS-7050T-36-F
- DCS-7050T-36-R
- DCS-7050T-52-F
- DCS-7050T-52-R
- DCS-7050T-52-SSD-F
- DCS-7050T-52-SSD-R
- DCS-7050T-64-F
- DCS-7050T-64-R
- DCS-7050T-64-SSD-F
- DCS-7050T-64-SSD-R
- DCS-7050TX-96-SSD-F
- DCS-7050TX-96-SSD-R
- DCS-7050TX-128-F
- DCS-7050TX-128-R
- DCS-7050TX-128-SSD-R
- DCS-7050TX-128-SSD-F
- DCS-7050TX2-128-F
- DCS-7050TX2-128-R
- DCS-7060CX-32S-F
- DCS-7060CX-32S-R
- DCS-7060CX-32S-SSD-F
- DCS-7060CX-32S-SSD-R
- DCS-7060CX2-32S-F
- DCS-7060CX2-32S-R
- DCS-7150S-24-F
- DCS-7150S-24-R
- DCS-7150S-24-CL-F
- DCS-7150S-24-CL-R
- DCS-7150S-24-CL-SSD-F
- DCS-7150S-24-CL-SSD-R
- DCS-7150S-52-CL-F
- DCS-7150S-52-CL-R
- DCS-7280QR-C72-R
- DCS-7280QR-C72-M-F
- DCS-7280QR-C72-M-R
- DCS-7280SR-48C6-F
- DCS-7280SR-48C6-R
- DCS-7280SR-48C6-M-F
- DCS-7280SR-48C6-M-R
- DCS-7280TR-48C6-F
- DCS-7280TR-48C6-R
- DCS-7280TR-48C6-M-F
- DCS-7280TR-48C6-M-R
- DCS-7280CR-48-F
- DCS-7280CR-48-D
- DCS-7280CR-48-DC-F
- DCS-7280SR2-48YC6-F
- DCS-7280SR2-48YC6-R
- DCS-7280SR2-48YC6-M-F
- DCS-7280SR2-48YC6-M-R
- DCS-7280SRA-48C6-F
- DCS-7280SRA-48C6-R
- DCS-7280SRA-48C6-M-F
- DCS-7280SRA-48C6-M-R

- DCS-7050QX-32S
- DCS-7050QX2-32S
- DCS-7050QX-32
- DCS-7050SX-64-F
- DCS-7050SX-64-R
- DCS-7050SX-64-SSD-F
- DCS-7050SX-64-SSD-R
- DCS-7050SX-72-F
- DCS-7050SX-72-R
- DCS-7050SX-72-SSD-F
- DCS-7050SX-72-SSD-R
- DCS-7050SX-96-F
- DCS-7050SX-96-R
- DCS-7050SX-96-SSD-F
- DCS-7050SX-96-SSD-R
- DCS-7050SX-128-F
- DCS-7050SX-128-R
- DCS-7050SX-128-SSD-F
- DCS-7050SX-128-SSD-R
- DCS-7050SX2-72Q-F
- DCS-7050SX2-72Q-R
- DCS-7050SX2-128-F
- DCS-7050SX2-128-R
- DCS-7050TX-48-F
- DCS-7050TX-48-R
- DCS-7050TX-48-SSD-F
- DCS-7050TX-48-SSD-R
- DCS-7050TX-64-F
- DCS-7050TX-64-R
- DCS-7050TX-64-SSD-R
- DCS-7050TX-64-SSD-F
- DCS-7050TX-72-F
- DCS-7050TX-72-R
- DCS-7050TX-72-SSD-F
- DCS-7050TX-72-SSD-R
- DCS-7050TX-96-F
- DCS-7050TX-96-R
- DCS-7150S-52-CL-SSD-F
- DCS-7150S-52-CL-SSD-R
- DCS-7150S-64-CL-F
- DCS-7150S-64-CL-R
- DCS-7150-64-CL-SSD-F
- DCS-7150-64-CL-SSD-R
- DCS-7160-32CQ-F
- DCS-7160-32CQ-R
- DCS-7160-32CQ-SSD-F
- DCS-7160-32CQ-SSD-R
- DCS-7160-48YC6-F
- DCS-7160-48YC6-R
- DCS-7160-48TC6-F
- DCS-7160-48TC6-R
- DCS-7250QX-64-F
- DCS-7250QX-64-R
- DCS-7250QX-64-SSD-F
- DCS-7250QX-64-SSD-R
- DCS-7260CX-64-F
- DCS-7260CX-64-R
- DCS-7260CX-64-SSD-F
- DCS-7260CX-64-SSD-R
- DCS-7260QX-64-F
- DCS-7260QX-64-R
- DCS-7260QX-64-SSD-F
- DCS-7260QX-64-SSD-R
- DCS-7280SE-64-F
- DCS-7280SE-64-R
- DCS-7280SE-68-F
- DCS-7280SE-68-R
- DCS-7280SE-72-F
- DCS-7280SE-72-R
- DCS-7280QR-C36-F
- DCS-7280QR-C36-R
- DCS-7280QR-C36-M-F
- DCS-7280QR-C36-M-R
- DCS-7280QR-C72-F
- DCS-7280TRA-48C6-F
- DCS-7280TRA-48C6-R
- DCS-7280TRA-48C6-M-F
- DCS-7280TRA-48C6-M-R
- DCS-7280QRA-C36S-F
- DCS-7280QRA-C36S-R
- DCS-7280SR2A-48YC6-F
- DCS-7280SR2A-48YC6-R
- DCS-7280SR2A-48YC6-M-F
- DCS-7280SR2A-48YC6-M-R
- DCS-7020TR-48-F
- DCS-7020TR-48-R
- PWR-1100AC-F
- PWR-1100AC-R
- PWR-1900AC-F
- PWR-1900-DC-F
- PWR-1900-DC-R
- PWR-745AC-F
- PWR-745AC-R
- PWR-750AC-F
- PWR-750AC-R
- PWR-747AC-F
- PWR-747AC-R
- PWR-650AC
- PWR-460AC-F
- PWR-460AC-R
- PWR-460DC-F
- PWR-460DC-R
- PWR-500AC-F
- PWR-500AC-R
- PWR-500-DC-F
- PWR-500-DC-R
- FAN-7002H-F
- FAN-7000-F
- FAN-7000-R
- FAN-7000H-F
- FAN-7000H-R

Modular

- DCS-7508
- DCS-7504
- DCS-7504N
- DCS-7508N
- DCS-7512N
- 7500E-SUP
- 7500E-SUP-D
- 7500R-48S2CQ-LC
- 7500R2-36CQ-LC
- 7500R2-18CQ-LC
- 7500R2A-36CQ-LC
- 7500R2AK-36CQ-LC
- 7500R2AK-48YCQ-LC
- 7504E-FM
- 7308X-FM
- 7316X-FM
- 7320X-32C-LC
- 7324X-FM-F
- 7328X-FM-F
- 7304-S-FAN
- 7308-S-FAN

- 7500-SUP2
- 7500-SUP2-D
- 7500E-36Q-LC
- 7500E-72S-LC
- 7500E-48S-LC
- 7500E-48T-LC
- 7500E-12CM-LC
- 7500E-6C2-LC
- 7500E-12CQ-LC
- 7500E-6CFPX-LC
- 7500R-8CFPX-LC
- 7500R-36CQ-LC
- 7500R-36Q-LC
- 7500RM-36CQ-LC
- 7508E-FM
- 7508R-FM
- 7504R-FM
- 7512R-FM
- DCS-7304
- DCS-7308
- DCS-7316
- 7300-SUP
- 7300-SUP-D
- 7300X-32Q-LC
- 7300X-64S-LC
- 7300X-64T-LC
- 7304X-FM
- PWR-2900AC
- PWR-3KT-AC-RED
- PWR-3K-DC-RED
- PWR-3K-AC-F
- PWR-3K-AC-R
- PWR-2700-DC-F
- PWR-2700-DC-R
- FAN-7002-F
- FAN-7002-R
- DCS-7500R-8CFPX-LC
- 7516-SUP2
- 7516R-FM
- 7516N

Transceiver

- 100GBASE-SR4
- 100GBASE-AOC
- 100GBASE-CR4
- 100GBASE-LR4
- 100GBASE-LRL4
- 100GBASE-CWDM4
- 100GE-DWDM2
- CFP2-100GBASE-LR4
- CFP2-100GBASE-ER4
- CFP2-100GBASE-XSR10
- CFPX-100G-DWDM
- CFPX-200G-DWDM
- 40GBASE-AOC
- 40GBASE-CR4
- 40GBASE-LR4
- 40GBASE-PLR4
- 40GBASE-PLRL4
- 40GBASE-SR4
- 40GBASE-ER4
- 40GBASE-XSR4
- 40GBASE-LRL4
- 40GBASE-UNIV
- 40GBASE-SRBD
- 25GBASE-CR
- 25GBASE-SR
- 25GBASE-AOC
- 25GBASE-LR
- 10GBASE-AOC
- 10GBASE-CR
- 10GBASE-DWDM
- 10GBASE-DWDM-ZR
- 10GBASE-DWDM-T
- 10GBASE-ZR
- 10GBASE-ER
- 10GBASE-LR
- 10GBASE-LRL
- 10GBASE-SR
- 10GBASE-SRL
- 1000BASE-SX
- 1000BASE-LX
- 1000BASE-BX10-D
- 1000BASE-BX10-U
- 1000BASE-T

Picking compatible versions for MLAG ISSU Upgrade/ Downgrade

Upgrading/downgrading using the MLAG ISSU procedure, from release EOS-A.B.C to release EOS-D.E.F can be done in one or multiple phases.

1. If A.B.C is a compatible EOS version for D.E.F (refer to the A.B.X or D.E.X release table) then you can directly do MLAG ISSU using the D.E.F version by following the MLAG ISSU procedure. (A.B.C -> D.E.F).
   Example: The customer wants to upgrade from 4.12.10 to 4.15.4F. In the Release 4.15.X MLAG ISSU Table, the 4.15.4F version has 4.12.10 as a MLAG ISSU compatible version, so customer can directly do an MLAG ISSU upgrade from 4.12.10 to 4.15.4F.
2. If A.B.C doesn't exist in the list of compatible versions for D.E.F (refer to the A.B.X or D.E.X release table), then look for the A.B.Y version in D.E.F's ISSU compatible EOS versions, do MLAG ISSU upgrade/downgrade from A.B.C to A.B.Y and then do MLAG ISSU upgrade/downgrade to D.E.F by following MLAG ISSU procedure (A.B.C -> A.B.Y -> D.E.F). Here, Y can be greater than or less than C.
   Example: The customer wants to upgrade from 4.14.1F to 4.15.4F. In Release 4.15.X MLAG ISSU Table 4.15.4F version has 4.14.9F as MLAG ISSU compatible version and Release 4.14.X MLAG ISSU Table 4.14.9F has 4.14.1F as MLAG ISSU compatible version, so customer can do MLAG ISSU upgrade from 4.14.1F to 4.14.9F and then to 4.15.4F.
3. Look for an D.E.Z version that's MLAG ISSU compatible with both A.B.C and D.E.F. Do MLAG ISSU upgrade/downgrade from A.B.C to D.E.Z and then do MLAG ISSU upgrade/downgrade to D.E.F (A.B.C -> D.E.Z -> D.E.F). Here Z can be greater than or less than F.
   Example: The customer wants to upgrade from 4.14.7F to 4.15.4F. In Release 4.15.X MLAG ISSU Table 4.15.0F version has 4.14.7F as MLAG ISSU compatible version and 4.15.4F has 4.15.0F as MLAG ISSU compatible version, so customer can do MLAG ISSU upgrade from 4.14.7F to 4.15.0F and then to 4.15.4F.
4. Look for an G.H.I version that's MLAG ISSU compatible with both A.B.C and D.E.F. Do an MLAG ISSU upgrade/downgrade from A.B.C to G.H.I and then do Mlag ISSU upgrade/downgrade to D.E.F (A.B.C -> G.H.I -> D.E.F).
5. In a highly unlikely scenario, if any of the above procedures are not acceptable, MLAG ISSU can be achieved by picking multiple intermediate versions.

Release 4.19.X MLAG ISSU Table

EOS Version	Mlag ISSU compatible EOS versions
4.19.0F	4.16.6M-4.16.12M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F, 4.17.4M-4.17.7M, 4.18.0F, 4.18.1.1F, 4.18.2F, 4.18.2-REV2-FX.1, 4.18.3.1F
4.19.1F	4.16.6M-4.16.12M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F, 4.17.4M-4.17.7M, 4.18.0F, 4.18.1.1F, 4.18.2F, 4.18.2-REV2-FX.1, 4.18.3.1F, 4.19.0F
4.19.2F	4.16.6M-4.16.12M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F, 4.17.4M-4.17.7M, 4.18.0F, 4.18.1.1F, 4.18.2F, 4.18.2-REV2-FX.1, 4.18.3.1F, 4.19.0F-1F

Release 4.18.X MLAG ISSU Table

EOS Version	Mlag ISSU compatible EOS versions
4.18.0F	4.16.6M-4.16.9M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F
4.18.1F	4.16.6M-4.16.10M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F, 4.17.4M, 4.18.0F
4.18.1.1F	4.16.6M-4.16.10M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F, 4.17.4M, 4.18.0F, 4.18.1F
4.18.2F	4.16.6M-4.16.10M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F, 4.17.4M, 4.18.0F, 4.18.1F, 4.18.1.1F
4.18.3F	4.16.6M-4.16.10M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F, 4.17.4M, 4.18.0F, 4.18.1F, 4.18.1.1F 4.18.2F

Release 4.17.X MLAG ISSU Table

EOS Version	Mlag ISSU compatible EOS versions
4.17.0F	4.16.6M
4.17.1F	4.16.6M-4.16.7M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.17.0F
4.17.2F	4.16.6M-4.16.8M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.1F
4.17.3F	4.16.6M-4.16.9M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.2F
4.17.4M	4.16.6M-4.16.9M, 4.16.7FX-MLAGISSU-TWO-STEP, 4.16.8FX-MLAGISSU-TWO-STEP, 4.17.0F-4.17.3F

Release 4.16.X MLAG ISSU Table

EOS Version	Mlag ISSU compatible EOS versions
4.16.6M	4.16.7FX-MLAGISSU-TWO-STEP
4.16.7M	4.16.6M, 4.16.7FX-MLAGISSU-TWO-STEP
4.16.8M	4.16.6M-4.16.7M, 4.16.7FX-MLAGISSU-TWO-STEP - 4.16.8FX-MLAGISSU-TWO-STEP
4.16.9M	4.16.6M-4.16.8M, 4.16.7FX-MLAGISSU-TWO-STEP - 4.16.8FX-MLAGISSU-TWO-STEP
4.16.10M	4.16.6M-4.16.9M, 4.16.7FX-MLAGISSU-TWO-STEP - 4.16.8FX-MLAGISSU-TWO-STEP
4.16.7FX-MLAGISSU-TWO-STEP	4.9.11, 4.10.8.1, 4.11.12, 4.12.11, 4.13.16M, 4.14.14M, 4.15.0F-4.15.4F, 4.15.5M-4.15.7M, 4.16.6M, 4.16.7M, 4.17.0F
4.16.8FX-MLAGISSU-TWO-STEP	4.9.11, 4.10.8.1, 4.11.12, 4.12.11, 4.13.16M, 4.14.15M, 4.15.0F-4.15.4F, 4.15.5M-4.15.8M, 4.16.6M-4.16.8M, 4.17.0F-4.17.1F

Release 4.15.X MLAG ISSU Table

EOS Version	Mlag ISSU compatible EOS versions
4.15.0F	4.9.11, 4.10.8.1, 4.11.11, 4.12.10, 4.13.12M, 4.14.7M
4.15.1F	4.9.11, 4.10.8.1, 4.11.11, 4.12.10, 4.13.12M, 4.14.7M, 4.15.0F
4.15.2F	4.9.11, 4.10.8.1, 4.11.11, 4.12.10, 4.13.12M, 4.14.9M, 4.15.0F-4.15.1F
4.15.3F	4.9.11, 4.10.8.1, 4.11.11, 4.12.10, 4.13.12M, 4.14.9M, 4.15.0F-4.15.2F
4.15.4F	4.9.11, 4.10.8.1, 4.11.11, 4.12.10, 4.13.12M, 4.14.9M, 4.15.0F-4.15.3F
4.15.5M	4.9.11, 4.10.8.1, 4.11.11, 4.12.10, 4.13.12M, 4.14.10M, 4.15.0F-4.15.4F
4.15.6M	4.9.11, 4.10.8.1, 4.11.12, 4.12.11, 4.13.15M, 4.14.12M, 4.15.0F-4.15.4F, 4.15.5M
4.15.7M	4.9.11, 4.10.8.1, 4.11.12, 4.12.11, 4.13.16M, 4.14.13M, 4.15.0F-4.15.4F, 4.15.5M-4.15.6M
4.15.8M	4.9.11, 4.10.8.1, 4.11.12, 4.12.11, 4.13.16M, 4.14.13M, 4.15.0F-4.15.4F, 4.15.5M-4.15.7M
4.15.9M	4.9.11, 4.10.8.1, 4.11.12, 4.12.11, 4.13.16M, 4.14.15M, 4.15.0F-4.15.4F,4.15.5M-4.15.8M
4.15.10M	4.9.11, 4.10.8.1, 4.11.12, 4.12.11, 4.13.16M, 4.14.16M, 4.15.0F-4.15.4F,4.15.5M-4.15.9M

Resolved Caveats in 4.18.5M

General

- If the Arista ML2 driver times out while synchronizing with CVX while using the JSON API in ML2, CVX will not provision VLANs and VLAN-to-VNI mappings on switches.

  A mitigation action is to configure a large region sync timeout to reduce the probability that a synchronization times out. (224942)

Layer 3

- A BGP router with a dynamic peer group(s) configured may incorrectly reject incoming BGP peer connections. This is due to miscounting the number of dynamic peers established when processing multiple received BGP OPEN requests from the same remote peer. This results in limiting the number of dynamic peers allowed to be established below the actual limit. (228771)

DCS-7010T, DCS-7050X[2], DCS-7060X[2], DCS-7250X, DCS-7260X3 and DCS-7300[X] Series

- Rapid IGMP join/leave on multiple groups can cause momentary traffic loss on stable receivers in those groups. (221285)

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

DCS-7280SE and DCS-7500E Series

- When storm control is disabled, all unknown unicast traffic gets dropped after SandAcl restart (201023)

Known Software Caveats in 4.18.5M

General

- Due to the slow nature of writes to USB, when copying two large files (typically 200+ MB) back to back to the external USB, the copy of the second file can end up in an "uninterruptible" state waiting for I/O to complete, resulting in a kernel crash (33988)

- The SuperServer agent can restart unexpectedly if tcpdump sessions are configured and a link being captured on by one of the sessions flaps. (60515)

- 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)

- For interfaces undergoing maintenance by virtue of being part of a user configured/builtin unit being put under maintenance, "show maintenance" would not reflect the correct maintenance status of the interface. (141942)

Layer 3

- FHRP state may start flapping between Backup and Master and Fhrp Agent may restart while dealing with large number of Virtual IP addresses. This is seen at a scale of 20K virtual IPs or more. (182399)

- When route to RP is ECMP, MSDP SA messages are accepted from only one of the possible peers, not all.

  To accept the SA message from a different MSDP peer, please use: ip msdp default-peer <peer_id> <RP>. (190306)

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)

Multicast

- On PimReg agent restart, PimReg might restart again if some of the S,G routes are
  still registering to the RP. (203520)

DCS-7010T, DCS-7050X[2], DCS-7060X[2], DCS-7250X, DCS-7260X3 and DCS-7300[X] Series

- Control packets sent out through a SVI will have its VLAN priority/CoS value set to 0. (75527)

- 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

- 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)

- The Strata agent may restart. (135192)

- If the number of VTEPs and number of ports on VXLAN VLANs overflow the hardware capacity and then an SVI is configured on these VLANs, the forwarding agent may restart unexpectedly.

  The workaround is to either remove the SVI configuration on the VXLAN VLAN or clear the overflow condition by reducing the number of ports on VLANs with VXLAN enabled. (139203)

- If MLAG fast redirection is configured, there may be a traffic loss when an MLAG port channel is being brought up. The duration of a traffic loss may increase with the number of VLANs enabled on that port channel. (183415)

- Some of the MACs learnt over remote VXLAN VTEPs go missing in hardware and are never relearnt when a member in peer-link port channel is shut then unshut. (184732)

- Changing the platform routing table mode ('platform trident routing-table partition') followed by platform forwarding table mode ('platform trident forwarding-table partition') can cause continuous parity errors to show up on L3_ENTRY_IPV4_UNICAST table and traffic loss.

  A workaround is to toggle the platform forwarding table mode, this would recover the traffic. (212447)

- When a port channel with configured LACP fallback individual mode enters fallback
  state where all port channel members act as individual ports, the data may be
  improperly forwarded or dropped on these ports. (222969)

DCS-7010T Series

- When the CLI command "default interface" is given for an interface corresponding to a port with a 1000BASE-X transceiver, the link may not come up until a "shut/no shut" command sequence is issued for that interface. (70630)

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

DCS-7050 and DCS-7300 Series

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

DCS-7050X and DCS-7300 Series

- 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)
- Under heavily congested broadcast/multicast flooding scenarios, control packet received may be incorrectly discarded. (156736)
- (A1 silicon only) MPLS traffic gets incorrectly prioritized, causing other traffic on the same port to get dropped. (160269)
  SKUs Affected: DCS-7050QX-32
- Configuring "switchport dot1q ethertype" and VxLAN routing (creating SVIs for VxLAN VLAN) simultaneously is not supported. If routing "switchport dot1q ethertype" has been configured and routing for VxLAN VLAN needs to be enabled, the workaround is to remove "switchport dot1q ethertype" configuration and reload the switch. (164362)
- In an MLAG configuration, if the StrataL2 agent is restarted, traffic to MLAG interfaces may be double delivered by both switches.

  The workaround is to removing and re-apply the MLAG configuration. (164669)
- Altering the priority of transmit queues of a port will result in some traffic loss on that port. (194460)
- Having PFC Watchdog enabled on twenty-five or more interfaces, the Strata agent might restart when QoS maps are changed. (195248)

DCS-7050X2 and DCS-7300 Series

- IPv6 link-local multicast packets (including neighbor discovery packets) may not be forwarded to all the members of the VLAN when no IPv6 address is configured.

  The workaround is to disable IGMP snooping on the VLAN. (191854)

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

- A linecard may be detected erroneously as removed and re-inserted after a SSO switchover. (34907)

- 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)

- MAC mirroring ACLs do not match IPv6 packets. (137537)

- A fabric module with a memory failing can persistently cause packets to be dropped over the fabric. (151115)
  Series Affected: DCS-7500E and DCS-7500R Series

- On devices with AlgoMatch enabled, the 'platform arad tcam counters feature' command does not work. (169493)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- On a device with with a large number of active VLANs, shutting and unshutting many interfaces may cause the SandMcast agent to be restarted. (175529)

- Mirrored traffic is not subject to egress security ACLs which are applied to mirroring destination ports. (190637)

- Egress security ACLs only apply to routed IP traffic. (191753)

- The layer 2 forwarding agent may restart on a VXLAN MLAG setup, in rare cases, when a local mac moves behind a VTEP. (215130)

DCS-7280E and DCS-7500E Series

- 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)

- While running Tap Aggregation, toggling the link state of a port-channel member configured as a tap interface has a very brief period where MAC addresses can be learned. The effect is that any learned MAC addresses will then be dropped if the destination MAC matches these learned addresses.

To resolve this issue, the customer should clear the mac address table. (141496)

- 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 if this is the case is to perform a full reset of the forwarding chip the Ethernet interface is on, using the "show platform arad map interface <Ethernet interface name>" to determine the forwarding chip to reset (should have the format "AradX" or "AradX/Y") and then running 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)

DCS 7500 and DCS-7300 Series

- Sub-interface configuration may not be cleaned up if a line card in a slot is replaced by a different model line card. (178945)

Layer 2

- Configuring VLANs within a config session that are currently in use as internal VLANs may fail with the message that internal VLANs cannot be created, even if the VLAN would no longer be used as an internal VLAN once the config session is applied. (132550)
- During a config-replace operation, if the mac security profile on an interface is replaced by another profile, and if the original security profile has been modified, then mac security may no longer be enabled on that interface.
  Workaround : Remove the profile from the interface and reconfigure. (187897)

Limitations and Restrictions in 4.18.5M

General

- The CLI does not allow access to files whose names contain spaces. (539)
- EOS SDK-based applications must be run via the 'daemon' command configuration. They cannot be run directly from bash. (158431)

- EOS extension scripts and agents which do not use EOS-SDK will need to be modified to work in 4.16.6M and beyond. (158467)
- EOS swix extensions containing RPMs which were based out of or procured from Fedora distributions prior to Fedora 18 may fail to install due to dependency issues. Suggested workaround is to recreate the swix files with the corresponding RPMs from Fedora 18 distribution. (162325)
- Packets with size greater than MTU of egress interface will not honor directflow flows and may not be forwarded (180927)
- SSO is hitful with subinterfaces. Protocols running on subinterfaces may experience session flaps during SSO. (188070)
- When using EVPN VXLAN in MLAG environment the Mlag agent might crash when VXLAN interface is shutdown due to a race condition. There is no workaround for this issue. (193475)

Layer 3

- 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)
- BFD Echo functionality is not available on L2 Port-Channels with BFD RFC7130. (190418)

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)

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)

- In a clustered CVX deployment with HSC connected to an NSX controller using a SSL profile, the OVSDB connection can fail during a switchover if the CVX nodes are configured with a different SSL profile.

  A workaround is to ensure that the SSL profile used by HSC is identical across controllers. (214918)

DCS-7010T, DCS-7050X[2], DCS-7060X[2], DCS-7250X, DCS-7260X3 and DCS-7300[X] 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)

- A large ACL and PBR policy configuration that consumes all TCAM resources may not fit after doing a config-replace, ACL agent restart or switch reload. After performing a config-replace, ACL agent restart or a switch reload, it is possible that only the ACL or the PBR policy will be able to fit. (105667)
  Series Affected: DCS-7010T, DCS-7050 and DCS-7050X Series

- There may be a momentary traffic disruption every time the nexthop specified in a PBR policy resolves to a new desgination: affected packets may be forwarded by normal L3 lookup, or be dropped.

  The system will recover automatically; the PBR policy will return to route packets as per the new nexthop resolution momentarily. (105670)

- 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)
- IGMP snooping is not supported on Vxlan enabled VLANs. The multicast packets will always be flooded locally and to remote VTEPs. (110479)
- 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)
- Configuring "hardware access-list resource sharing vlan in" in a config replace session or in config session is not supported (114291)
  Series Affected: DCS-7010T 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-7010T and DCS-7050X Series
- IP ACLs configured on SVIs to match routed IP multicast traffic may also match bridged IP multicast traffic in that SVI. (152523)
- Mirroring of Vxlan encapsulated packets in the egress direction is not supported. (167189)
- When any PBR policy is applied, packets that violate the egress MTU and are destined to flood the VLAN will end up being flooded instead of being sent to the CPU. (196134)

DCS-7010T Series

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

- Enabling counters for Static or Twice NAT connection can cause FocalPointV2 agent restarts, when the number of connections exceed 275. (109048)

DCS-7060X and DCS-7300X Series

- Cut-through mode is not supported on the SFP+ interfaces. (182728)

DCS-7050X and DCS-7300 Series

- The mirroring to GRE Tunnel feature does not support sub-interfaces as egress interfaces. (136514)
- Packets sourced from the CPU to be VXLAN encapsulated will not have the right DSCP marking in the outer header based on the global QOS map configuration. (139248)
- Tcam entries used by IPv6 standard access list is not shared across interfaces (159827)
- In MLAG VTEP configuration, the switch incorrectly drops VXLAN encapsulated packets that are destined to the VTEP IP address but the peer switch's bridge MAC address. (159874)
- 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)
- 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)
- If an SVI is used as a core interface to reach remote Vteps, any L3 EVPN traffic using that SVI will be dropped if the underlay mac becomes unlearnt. A workaround is to configure MAC timeout to a higher value than ARP timeout to ensure macs don't get aged out. (192419)

DCS-7050X2 and DCS-7300 Series

- Egress IP/IPv6 router ACL is not supported for VXLAN encapsulated traffic. (148642)
- Egress VLAN translation will not work on routed multicast packets when the VLAN to be translated is part of the outgoing interface list. (151093)

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

- 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)

- Mirroring to GRE tunnels does not support GRE destinations that are reachable by sub-interfaces. (136130)

- IPv6 Egress ACL deny logging is not supported on subinterfaces. (146487)

- 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 interface. (151356)

- 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)

- While in Tap Aggregation mode with 802.1BR/VN-Tag stripping configured, IPv4 and IPv6 traffic steering rules are not supported on packets with more than one 802.1Q tag. (198514)

- Tap Aggregation features such as policy-based traffic steering 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

- Due to a hardware limitation, "show interfaces queue length" and LANZ may fail to report congestion in some scenarios, usually involving sFlow queues or multicast traffic. (199470)
  Series Affected: DCS-7280R, DCS-7280R2, DCS-7500R and DCS-7500R2 Series

- 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)

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)

DCS-7160 Series

- No support for matching on DSCP field on IPpackets 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)

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 networt-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.