Dell System S4810 9.11(0.0P9) Release Notes

This document contains information on open and resolved caveats, and operational information specific to the Dell Networking OS software and the S4810 platform.

Caveats are unexpected or incorrect behavior, and are listed in order of Problem Report (PR) number within the appropriate sections.

NOTE: Customers can subscribe to caveat update reports or use the BugTrack search tool to read current information about open and closed software caveats. To subscribe or use BugTrack, visit iSupport at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx. BugTrack currently tracks software caveats opened in Dell Networking OS version 6.2.1.1 and later. All Release Notes are available on the Software Center tab of iSupport. The link to the relevant Release Notes for each software version is next to the link for that version: https://www.force10networks.com/CSPortal20/Software/Downloads.aspx.

For more information on hardware and software features, commands, and capabilities, refer to the Dell Networking website at: https://www.dell.com/networking.

Current Version: 9.11(0.0P9)
Release Date: 2017-04-24
Previous Version: 9.11(0.0P8)

Topics:

Contents

Document Revision History

Table 1. Revision History

Date	Description
2017–04	Initial release.

Supported Brocade Cables

The following Brocade cables are supported with this platform:

Table 2. Supported Brocade Cables

Cable Description
CUS,PCT B-8000 10GbE TWINAX 3 METER 8PACK
CUS,PCT B-8000 10GbE TWINAX 5 METER 1PACK
CUS,PCT B-8000 10GbE TWINAX 5 METER 8PACK
CUS,PCT B-8000 10GbE TWINAX 1 METER 1PACK
CUS,PCT B-8000 10GbE TWINAX 1 METER 8PACK
CUS,PCT B-8000 10GbE TWINAX 3 METER 1PACK

Supported Hardware

The following hardware is supported with this platform:

Table 3. Supported Hardware

Hardware
48 port 10G SFP+ ports with 4 QSFP+ 40G ports
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 DC power supply and 2 fan subsystem with airflow from I/O side to power supply unit (PSU) side

Hardware
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 AC power supply and 2 fan subsystem with airflow from I/O side to power supply unit (PSU) side
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 DC power supply and 2 fan subsystem with airflow from power supply unit (PSU) side to I/O side
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 AC power supply and 2 fan subsystem with airflow from power supply unit (PSU) side to I/O side
S4810 Series – Fan with airflow from I/O side to power supply unit (PSU) side
S4810 Series – Fan with airflow from PSU side to I/O side
S4810 Series – DC Power supply with airflow from I/O side to power supply unit (PSU) side
S4810 Series – DC power supply with airflow from power supply unit (PSU) side to I/O side
S4810 Series – AC Power supply with airflow from I/O side to power supply unit (PSU) side
S4810 Series – AC Power supply with airflow from power supply unit (PSU) side to I/O side

NOTE: Fan Modules and Power supplies (PSUs) are field replaceable units. Dell Networking does not support a mix of power supply types (i.e., AC and DC) in the same switch.

NOTE: All fans and PSUs must have the same airflow direction. Should a mixed airflow configuration happen, the switch detects the discrepancy and performs a shutdown, if the module is not replaced within few minutes.

NOTE: Due to hardware limitation, 1G Cu SFP with QSA is not supported.

New Dell Networking OS Version 9.11(0.0) Features

The following features have been added to the S4810 with Dell Networking OS version 9.11(0.0):

Feature	Description
802.1x re-authentication	The re-authentication is applicable for authenticated 802.1x devices. When there is a change in the authentication servers, the supplicants connected to all the ports are forced to re-authenticate.
AAA re-authentication	Enable re-authentication of user whenever there is a change in the authentication.
Ability to configure GRE protocol type in ERPM	Introduced an option to configure GRE protocol type in ERPM.
Ability to mirror PFC pause frames in RX direction	Support to mirror PFC pause frames in RX direction.
BFD over static route	Support to selectively enable or disable BFD on specific next hops based on the configured static route.
BGP peer shutdown	Introduced support for shutting down BGP neighbors across all address families and individual address families.
ECMP group count	The show cam-usage command now displays the amount of used and available CAM space for ECMP groups in each CAM partition.
FRRP support on VLT	Support for inter-connecting VLT domains across data centers using FRRP ring through VLTi.

Global rate interval configuration	Ability to configure rate-interval globally. This configuration replaces the default rate-interval value of all physical and portchannel interfaces from its default value to the new configured value.
ICMP vulnerabilities	Introduced support to drop icmpv4 or icmpv6 reply messages.
IP PIM RP Candidate	Support for configuring a PIM router to act as an RP for a specific set of multicast group address.
MIB support to display the available partitions on flash	Introduced MIB objects to display the information corresponding to various partitions such as / flash, /tmp, /usr/pkg, and /f10/Conf.
MIB support to entAliasMappingTable and LAG	Introduced MIB objects to retrieve the configured LACP information. Introduced MIB objects to map the physical interfaces to its corresponding ifIndex value.
Monitoring transceiver data through SNMP	Introduced a new MIB to retrieve transceiver details.
Multicast traceroute	Support for multicast traceroute (mtrace). mtrace is a multicast diagnostic facility used for tracing multicast paths.
OSPF throttling	Support for specifying SPF timer values in milli seconds.
Secured CLI mode	Introduced the secured CLI mode to prevent users from enhancing the permissions or promoting the privilege levels.
Show QoS Statistics to show egress per queue per Interface drop rate and per queue per port TX rate	Enhanced the show qos statistics egress-queue command output to display per-queue per-port TX and drop rates. Added MIB support to retrieve the same information using SNMP.
SNMP supoprt for WRED drop counters	Introduced MIB support for green, yellow, and red drop counters.
SupportAssist enhancements	SupportAssist is enabled by default and can be disabled using CLI. When SupportAssist is enabled, the switch periodically sends information to an external SupportAssist server. The information sent includes the identity of the switch like service tag and serial number, configuration, logs, status, and diagnostic information. Dell Networking OS 9.11(0.0) introduces support for transferring core files and event logs to the SupportAssist server.
Two-factor authentication	Introduced two-factor authentication (2FA) in RADIUS deployments to enhance security.
Viewing uRPF status	Enhanced the show ipv4 interface and show ipv6 interface commands to display unicast reverse path forwarding (uRPF) status.
VLT port monitoring	Introduced support for remote port-monitoring (RSPAN) with VLT.
VRRP priority 255	Introduced support for VRRP Priority 255 in the VLT environment.
X.509v3	Support for X.509v3 Digital Certificates on Dell Networking OS.

Restrictions

If an Intel X520 CNA adapter is used as an FCoE initiator, follow these steps to establish FCoE sessions to send and receive traffic on an S4810 switch:

1 On the server, uninstall the old Intel driver (version 13.0.0 or older).

2 Re-install the Intel driver using version 13.5 A00 (or later) from the http://www.dell.com website.Important: During the installation, do not select the ISCSI part of the driver; select only the FCoE check box.

3 On each server-facing port, enter the following commands in interface configuration mode. The dcbx version cee command configures a port to use the CEE (Intel 1.01) version of DCBX. Configure server-facing ports with the shutdown and no shutdown commands as needed. For example:

```
Dell# interface tenGigabitEthernet 0/1
Dell(conf-if-te-0/1)# portmode hybrid
Dell(conf-if-te-0/1)# switchport
Dell(conf-if-te-0/1)# protocol lldp
Dell(conf-lldp)# dcbx port-role auto-downstream
Dell(conf-lldp)# dcbx version cee
Dell(conf-lldp)# exit
Dell(conf-if-te-0/1)# spanning-tree pvst edge-port
Dell(conf-if-te-0/1)# no shutdown
Dell(conf-if-te-0/1)# exit
Dell#
```

4 Display information on FIP-snooped sessions and check the entries in ENode Interface fields to see if you have established the FCoE session on a server-facing port.

show fip-snooping sessions

EXEC Privilege

- The following features are not available in the Dell Networking OS from version 9.7(0.0):
  - PIM ECMP
  - Static IGMP join (`ip igmp static-group`)
  - IGMP querier timeout configuration (`ip igmp querier-timeout`)
  - IGMP group join limit (`ip igmp group join-limit`)
- If you use the `interface range` command to select multiple interfaces that are added to the management VRF, the `ipv6 address` command does not display the `autoconfig` option. You can configure the `autoconfig` command on individual interfaces.
- If you use the `interface range` command to select multiple interfaces that are added to the management VRF, the `ipv6 nd` command displays the following options but they do not take effect if you use them:
  - dns-server
  - hop-limit
  - managed-config-flag
  - max-ra-interval
  - mtu
  - other-config-flag
  - prefix
  - ra-guard
  - ra-lifetime
  - reachable-time
  - retrans-timer
  - suppress-ra

Changes to Default Behavior and CLI Syntax

The following behavior and CLI changes are applicable to the S4810 switch with Dell Networking OS version 9.11(0.0):

While configuring a password using the command line interface, the ~ character is supported.

S4810 Upgrade Procedures: Overview

To upgrade the Dell Networking OS to version 9.11(0.0) on a S4810 switch, complete these steps:

- Upgrading the S4810 Dell Networking OS Image and Boot Code
- Upgrading the CPLD
- VLT Upgrade Procedure

Upgrading the S4810 Dell Networking OS Image and Boot Code

The S4810 system is pre-loaded with default Dell Networking OS software.

NOTE: Before upgrading Dell Networking OS on S4810 from a version prior to 8.3.12.0 to version 9.11(0.0), ensure to increase the partition size by upgrading to version 8.3.12.0.

NOTE: If the upgrade image is greater than 32MB in size, switches running Dell Networking OS version prior to 9.1(0.0) do not support software upgrade using TFTP. Use FTP, SCP, FLASH, or NFSMOUNT instead. Dell Networking OS Version 9.1(0.0) introduced TFTP enhancements to support file transfers larger than 32MB.

NOTE: If VLT configurations exist on a switch that runs Dell Networking OS version 9.2(0.0) or prior, ensure that all switches in the VLT domain are upgraded to version 9.3(0.0) before upgrading to version 9.11(0.0).

NOTE: You can directly upgrade a switch that runs Dell Networking OS version 8.3.12.0 (or later) to version 9.11(0.0), if VLT configurations do not exist on that switch.

Bare Metal Provisioning

NOTE: If you are using Bare Metal Provisioning (BMP), refer to the Bare Metal Provisioning chapter in the Dell Networking OS Configuration Guide or the Open Automation Guide.

Manual Upgrade Procedure

Follow these steps to upgrade your S4810 system:

1 Dell Networking recommends that you back up your startup configuration and any important files and directories to an external media prior to upgrading the system.

2 Upgrade the Dell Networking OS in flash partition A: or B:

upgrade system [flash: | ftp: | scp: | tftp:] [A: | B:]

EXEC Privilege

```
Dell#upgrade system ftp: a:
Address or name of remote host []: 10.16.127.35
Source file name []: FTOS-SE-9.11.0.0.bin
User name to login remote host: ftpuser
Password to login remote host:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Erasing Sseries Primary Image, please wait
.....
.....
.....
.....
.....
.....
.....
.....Writing .....
.....
.....
.....
```

```
.............................................................................................
.............................................................................................
.............................................................................................
.............................................................................................
.........................
.............................................................................................
.!
44220292 bytes successfully copied
System image upgrade completed successfully.
Dell #
```

3 In case of a stack setup, upgrade the Dell Networking OS for the stacked units.

upgrade system stack-unit [0-11 | all] [A: | B:]

EXEC Privilege

If A: is specified in the command, the Dell Networking OS version present in Management unit's A: partition will be pushed to the stack units. If B: is specified in the command, the Management unit's B: will be pushed to the stack units. Upgrade of stack units can be done on individual units by specifying the unit id [0-11] or on all units by using all in the command.

```
Dell#upgrade system stack-unit all A:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image upgraded to all
Dell#
```

4 Verify the Dell Networking OS has been upgraded correctly in the upgraded flash partition

show boot system stack-unit [0-11 | all]

EXEC PRIVILEGE

The Dell Networking OS versions present in A: and B: can be viewed for individual units by specifying the stack unit id [0-11] in the command or for all the stack units by specifying all in the command.

```
Dell#show boot system stack-unit all

Current system image information in the system:
===============================================

Type                        Boot Type       A                B
---------------------------------------------------------------------
Stack-unit 0                  FLASH BOOT    9.11(0.0)     9.10(0.0)  [boot]
Stack-unit 1                  FLASH BOOT    9.11(0.0)     9.10(0.0)  [boot]
Stack-unit 2 is not present.
Stack-unit 3 is not present.
Stack-unit 4 is not present.
Stack-unit 5 is not present.
Stack-unit 6 is not present.
Stack-unit 7 is not present.
Stack-unit 8 is not present.
Stack-unit 9 is not present.
Stack-unit 10 is not present.
Stack-unit 11 is not present.
Dell#
```

5 Upgrade the S4810 Boot Code.

upgrade boot [flash: | ftp: | scp: | tftp:]

EXEC Privilege

Dell Networking OS version 9.11(0.0) requires S4810 Boot Code version 1.2.0.5. If any higher versions of Boot Code are present in the unit, do not upgrade the Boot Code.

```
Dell#upgrade boot ftp:
Address or name of remote host []: 10.16.127.35
Source file name []: U-boot.1.2.0.5.bin
User name to login remote host: ftpuser
Password to login remote host:
!
Erasing SSeries BootImageUpgrade Table of Contents, please wait
.!........Writing ................................!
524528 bytes successfully copied
Dell#
```

6 In case of a stack setup, upgrade the S4810 Boot Code to the stack units.

upgrade boot stack-unit [0-11 | all]

EXEC Privilege

The S4810 Boot Code can be upgraded to individual units by specifying the stack unit ID [0-11] in the command or it can be upgraded on all stack units by specifying all in the command.

```
Dell#upgrade boot stack-unit all
!!!!!!!!!!
Dell#
```

7 Change the Primary Boot Parameter of the S4810 to the upgraded partition A: or B:

boot system stack-unit [0-11 | all] primary [system A: | system B: | tftp://URL]

CONFIGURATION

8 Save the configuration so that the configuration will be retained after a reload using write memory command.

write memory

EXEC PRIVILEGE

In case of a stack setup, the configuration will be saved in the Management as well as the Standby units.

```
Dell#write memory
!
Synchronizing data to peer Stack-unit
!!!!!!!!
Dell#
```

9 Reload the unit

reload

EXEC PRIVILEGE

```
Dell#reload

Proceed with reload [confirm yes/no]: yes
Dec 2 21:32:27: %STKUNIT0-M:CP %CHMGR-5-RELOAD: User request to reload the chassis
syncing disks... done
```

10 Verify the S4810 has been upgraded to the Dell Networking OS version 9.11(0.0).

show version

EXEC PRIVILEGE

```
Dell#show version
Dell Real Time Operating System Software
Dell Operating System Version:  2.0
Dell Application Software Version:  9.11(0.0)
```

```
Copyright (c) 1999-2016 by Dell Inc. All Rights Reserved.
Build Time: Fri Dec  2 16:58:02 2016
Build Path: /build/build02/SW/SRC
Dell Networking OS uptime is 2 minute(s)

System image file is "system://A"

System Type: S4810
Control Processor: Freescale QorIQ P2020 with 2 Gbytes (2147483648 bytes) of memory, core(s)
1.

128M bytes of boot flash memory.

  1 52-port GE/TE/FG (SE)
 48 Ten GigabitEthernet/IEEE 802.3 interface(s)
  4 Forty GigabitEthernet/IEEE 802.3 interface(s)
Dell#
```

11 Verify the S4810 has been upgraded to the latest Boot Code

show system stack-unit [0-11]

EXEC PRIVILEGE

```
Dell#show system stack-unit 0

--  Unit 0 --
Unit Type                  : Management Unit
Status                     : online
Next Boot                  : online
Required Type              : S4810 - 52-port GE/TE/FG (SE)
Current Type               : S4810 - 52-port GE/TE/FG (SE)
Master priority            : 0
Hardware Rev               : 3.0
Num Ports                  : 64
Up Time                    : 2 min
Dell Networking OS Version : 9.11(0.0)
Jumbo Capable              : yes
POE Capable                : no
FIPS Mode                  : disabled
Boot Flash                 : 1.2.0.5
```

SSH — SSH host keys are stored in NVRAM. Dell Networking OS regenerates them when Dell Networking OS applies the startup-config and the ip ssh server enable configuration. However, if the SSH client has "Strict Host Key" checking enabled, the SSH client denies access to the Dell Networking OS SSH server. To resolve this issue, you must modify the SSH client settings so that it uses the new key.

SMARTSCRIPTS

To uninstall and install new SMARTSCRIPTS packages after upgrading to Dell Networking OS version 9.11(0.0), refer to the Open Automation Guide - 9.11(0.0).

Upgrading the CPLD

The S4810 system with Dell Networking OS version 9.11(0.0) or later requires CPLD image 7.

Verify that a CPLD upgrade is required

Use the following command to identify the CPLD version loaded in the device:

```
Dell#show revision
--  Stack unit 0  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)
```

```
--  Stack unit 1  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)

--  Stack unit 2  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)

Dell#
```

Use the following command to view CPLD version that is associated with the Dell Networking OS image:

```
Dell#show os-version

RELEASE IMAGE INFORMATION :
------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
S-Series:  SE         9.11(0.0)          44220292      Dec  2 2016 17:24:13

TARGET IMAGE INFORMATION :
------------------------------------------------------------------------
        Type          Version       Target                          checksum
     runtime         9.11(0.0)             Control Processor       passed

CPLD IMAGE INFORMATION :
------------------------------------------------------------------------
         Card                       CPLD Name    Version
Stack-unit 0              S4810 SYSTEM CPLD          7
Stack-unit 1              S4810 SYSTEM CPLD          7
Stack-unit 2              S4810 SYSTEM CPLD          7
```

Upgrading the CPLD Image

NOTE: The upgrade fpga-image stack-unit {0-11} booted command is hidden when using the FPGA Upgrade feature in the CLI. However, it is a supported command and will be accepted when entered as documented.

To upgrade the CPLD image on the S4810:

1 Shut down all of the interfaces on the system.

shutdown

INTERFACE

2 Upgrade the CPLD image.

upgrade fpga-image stack-unit [0-11] booted

EXEC Privilege

```
Dell# upgrade fpga-image stack-unit 0 booted

Current information for the system:
=====================================

  Card                    Device Name    Current Version     New Version
-------------------------------------------------------------------------
 Unit0              S4810 SYSTEM CPLD                 7               7

    **********************************************************************
    *  Warning - Upgrading FPGA is inherently risky and should           *
    *  only be attempted when necessary.  A failure at this upgrade may  *
    *  cause a board RMA.  Proceed with caution !                        *
    **********************************************************************
```

```
Upgrade image for stack-unit 0 [yes/no]: yes


FPGA upgrade in progress!!! Please do NOT power off the unit!!!
!!Dec 2 16:06:40: %S4810:0 %DOWNLOAD-6-FPGA_UPGRADE: stack-unit 0 fpga upgrade success.


Upgrade result :
================
Unit 0 FPGA upgrade successful Unit 0. will go for reboot to complete the upgrade.
Dell#
```

3 Check whether the CPLD has been upgraded to the latest version.

show revision

EXEC PRIVILEGE

```
Dell#show revision

--  Stack unit 0  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)

--  Stack unit 1  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)

--  Stack unit 2  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)
Dell#
```

VLT Upgrade Procedure

To upgrade the Dell Networking OS in a VLT setup from version 9.2(0.0) to the latest version, upgrade Dell Networking OS to version 9.3(0.0) first and then to the newer version. If you are already running Dell Networking OS version 9.3(0.0) or later, you can directly upgrade the Dell Networking OS to the latest version. To upgrade the Dell Networking OS, on systems running VLT, perform the following steps:

1 Upgrade the system-flash partition A or B with the new image on both VLT peers.On both the VLT peers, set Primary boot parameter to boot the system from upgraded system flash partition [A or B].You can enter one of the following options:**flash** — Copies from flash file system (flash://filepath).**ftp** — Copies from remote file system (ftp://userid:password@hostip//filepath).**scp** — Copies from remote file system (scp://userid:password@hostip//filepath).**tftp** — Copies from remote file system (tftp://hostip/filepath).

upgrade system [flash: | ftp: | scp: | tftp: | usbflash:] [A: | B:]

EXEC Privilege

2 Reload or power-cycle one of the VLT peers (For Example, Peer 2).

reload or power cycle

3 Wait for Peer 2 to come up; VLT adjacency will be established. (Peer 2 - new image and Peer 1 - old image).

> **NOTE: Between software versions 8.3.10.0 & 9.4P1 both VLT peers are running different VLT versions, a VLT peering will not established.**

4 Wait for the Peer 2 to bring up all VLT LAG ports. Use the command **show vlt detail** to confirm all VLT ports in the local chassis are active.

show vlt detail

EXEC Privilege

5 Following upgrade, use the **write memory** command to save the running-config to memory.

write memory

EXEC Privilege

6 Ensure both the nodes are now forwarding traffic.

NOTE:

- When you upgrade VLT nodes from 8.3.12 to 9.11.0.0, 9.1 to 9.11.0.0, 9.2 to 9.11.0.0, 9.3 to 9.11.0.0, 9.4 to 9.11.0.0, 9.5 to 9.11.0.0, 9.6 to 9.11.0.0, 9.7 to 9.11.0.0, 9.8 to 9.11.0.0, 9.9 to 9.11.0.0, and 9.10 to 9.11.0.0, forwarding traffic is not affected.
- If you upgrade VLT nodes from 8.3.10.0 to 9.x.x.x, layer 2 switched packets are flooded until all MAC addresses are learned. Layer 3 routed packets are dropped until all ARP entries are resolved and routes are learned due to version mismatch.

Layer 2 switched packets will be flooded until all MACs are learned and Layer 3 routed packets will be dropped until all ARPs are resolved and routes are learned due to version mismatch.

7 When all VLT ports are active on the Peer 2, repeat steps 2 through 5 for the Peer 1.

NOTE: After upgrading to the latest Dell Networking OS version, upgrade the CPLD if required.

Documentation Corrections

This section describes the error identified in the current releases of the Dell Networking OS.

- The *Dell Configuration Guide for the S6000-ON System* and *Dell Command Line Reference Guide for the S6000-ON System* mention that the system supports up to eight ACL VLAN groups. But the system supports up to 31 ACL VLAN groups.
- The *Dell Networking OS Command Line Reference Guide* incorrectly mentions a note on multi-process OSPF. It will be corrected in the next release by including the following note:
  - The Dell Networking OS versions 9.4(0.0) and 9.7(0.0) introduce support for VRF on OSPFv2 and OSPFv3 respectively. The multi-process OSPF feature supported on Dell Networking OS version 7.8.1.0 is modified. In earlier versions, multiple OSPF processes were created without VRF (prior to 9.4(0.0)). In the Dell Networking OS versions 9.4(0.0) and 9.7(0.0) (for OSPFv3), multiple OSPF processes can be created on a router, but with only one OSPF process per VRF. However, there can be one OSFPv2 and one OSPFv3 on the same VRF.
- The following note will be added to *Open Shortest Path First (OSPFv2 and OSPFv3)* topic of the *Dell Networking OS Command Line Reference Guide*:
  - OSPFv2 is supported on IPv6 tunnels only and OSPFv3 is supported on IPv4 tunnels only.
- The following Usage Information will be added to `router ospf` command of the *Dell Networking OS Command Line Reference Guide*:
  - You can create only one OSPFv2 process per VRF.
- When FRRP is enabled in a VLT domain, no flavor of Spanning tree should concurrently be enabled on the nodes of that specific VLT domain. In essence FRRP and xSTP should not co-exist in a VLT environment.

Deferred Issues

Issues that appear in this section were reported in Dell Networking OS version 9.11(0.0) as open, but have since been deferred. Deferred caveats are those that are found to be invalid, not reproducible, or not scheduled for resolution.

Deferred S4810 9.11(0.0) Software Issues

The following caveats are deferred in Dell Networking OS version 9.11(0.0)

IP Stack (Deferred)

PR# 161657

Severity:	Sev 2
Synopsis:	When ND entries are deleted in one of the VLT peer, it is not synced to other VLT peer.
Release Notes:	If ND in VLT-Node-1 ND is deleted, it is not synced to VLT-Node-2. But as soon as node-1 learns ND again due to any pkt being received for that station it will be synced to node-2. Since traffic is hashed across both nodes the time will be less.

Workaround:	"Clear ipv6 neighbor" command could be used to remove stale entries.

Fixed Issues

Fixed issues are reported using the following definitions.

Category	Description
PR#	Problem Report number that identifies the issue.
Severity	**S1** — Crash: A software crash occurs in the kernel or a running process that requires a restart of AFM, the router, switch, or process. **S2** — Critical: An issue that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no work-around acceptable to the customer. **S3** — Major: An issue that affects the functionality of a major feature or negatively effects the network for which there exists a work-around that is acceptable to the customer. **S4** — Minor: A cosmetic issue or an issue in a minor feature with little or no network impact for which there might be a work-around.
Synopsis	Synopsis is the title or short description of the issue.
Release Notes	Release Notes description contains more detailed information about the issue.
Work around	Work around describes a mechanism for circumventing, avoiding, or recovering from the issue. It might not be a permanent solution. Issues listed in the "Closed Caveats" section should not be present, and the work-around is unnecessary, as the version of code for which this release note is documented has resolved the caveat.

Fixed S4810 9.11(0.0P9) Software Issues

The following issues have been resolved in the Dell Networking OS version 9.11(0.0P9):

PR# 157308	
Severity:	Sev 2
Synopsis:	In a BGP OPEN message, if the capability attribute is empty, then BGP updates are not installed on the switch.
Release Notes:	In a BGP OPEN message, if the capability attribute is empty, then BGP updates are not installed on the switch.
Workaround:	None.
PR# 161297	
Severity:	Sev 2

Synopsis:	Router advertisement (RA) flooding on a layer 3 IPv6 interface causes the system to reboot.
Release Notes:	The system experiences a software exception when a layer 3 IPv6 interface is flooded with too many router advertisements.
Workaround:	None.

Fixed S4810 9.11(0.0P8) Software Issues

The following issues have been resolved in the Dell Networking OS version 9.11(0.0P8):

PR# 162254

Severity:	Sev 2
Synopsis:	With BFD configured, static route stays up even though the next-hop is unreachable.
Release Notes:	With BFD configured, static route stays up even though the next-hop is unreachable. In this scenario, the next-hop is unreachable due to the removal of the IP address by the neighbor.
Workaround:	None.

PR# 162464

Severity:	Sev 1
Synopsis:	In certain scenarios, the LSA delay origination timer is set to a very high value.
Release Notes:	In certain scenarios, the LSA delay origination timer is set to a very high value. This causes a very long delay to the originating LSA and this results in removal of routes. The large delay is shown in the BACKOFF transmit logs with either a negative or large timer.
Workaround:	None.

PR# 162484

Severity:	Sev 3
Synopsis:	VLT mismatch occurs when the private VLANS are configured on the system.
Release Notes:	When secondary VLANs are configured on both local and peer VLT devices, VLT mismatch occurs on the local system.
Workaround:	None.

PR# 162736

Severity:	Sev 2
Synopsis:	After passing through the switch, DHCPv6 packets have extra 4 bytes.

Release Notes:	After passing through the switch, DHCPv6 packets have extra 4 bytes.
Workaround:	None.
PR# 162737	
Severity:	Sev 1
Synopsis:	In certain scenarios, duplicate address and routing loop issues are observed because of stale routes in the kernel.
Release Notes:	In certain scenarios, the system cannot remove routes with a different prefix, from the kernel. This causes stale routes which causes the duplicate address and routing loop issues.
Workaround:	None.
PR# 162783	
Severity:	Sev 2
Synopsis:	In certain scenarios, `passive-interface default` command is not added under the OSPF configuration.
Release Notes:	In certain scenarios, `passive-interface default` command is not added under the OSPF configuration.
Workaround:	Remove the `passive-interface default` configuration and then re-apply it.

Fixed S4810 9.11(0.0P4) Software Issues

The following issues have been resolved in the Dell Networking OS version 9.11(0.0P4):

PR# 153839	
Severity:	Sev 1
Synopsis:	Incorrect counter increments corresponding to the protocol queue causes the system to reload.
Release Notes:	Incorrect counter increments corresponding to the protocol queue causes the system to reload.
Workaround:	None.
PR# 158503	
Severity:	Sev 2
Synopsis:	In certain scenarios, the SSH process remains active even after the session is closed, causing high CPU usage.
Release Notes:	In certain scenarios, the SSH process remains active even after the session is closed, causing high CPU usage.

Workaround:	None.
PR# 160879	
Severity:	Sev 1
Synopsis:	Connecting to the switch frequently using telnet can cause the device to reboot.
Release Notes:	The system may experience a software exception and reboot if connected through telnet or SSH very frequently.
Workaround:	Decrease the frequency of telnet or SSH connections.
PR# 160890	
Severity:	Sev 3
Synopsis:	The DHCP client, does not get the IP address.
Release Notes:	When DHCP snooping is enabled on the second-hop router from the DHCP client, the client does not get the IP address.
Workaround:	NA
PR# 161181	
Severity:	Sev 2
Synopsis:	Communication failures happen in some of the member units.
Release Notes:	In certain rare scenarios, after the stack failover, communication failures happen in some of the member units.
Workaround:	None
PR# 161408	
Severity:	Sev 2
Synopsis:	When the cam-ipv6 extended-prefix command is configured, the used value in the show cam-usage command output is incorrect.
Release Notes:	When the cam-ipv6 extended-prefix command is configured, the used value in the show cam-usage command output is incorrect for the ipv6 routes with prefixes from 0/65 to 0/127.
Workaround:	None
PR# 161752	
Severity:	Sev 2
Synopsis:	The system displays a configuration error when resume-offset is configured to be higher than pause-threshold.
Release Notes:	The system displays a configuration error when resume-offset is configured to be higher than pause-threshold.

Workaround:	Set the pause-threshold higher than or equal to the resume-offset.
PR# 161761	
Severity:	Sev 2
Synopsis:	BFD session goes down, when a new MAC address is received for the existing session.
Release Notes:	BFD session goes down, when a new MAC address is received for the existing session.
Workaround:	Remove and add the static route configuration.
PR# 161785	
Severity:	Sev 1
Synopsis:	CRC errors seen with mellanox when connected with DAC cables of length >= 4m
Release Notes:	40G DAC cables of length greater than or equal to 4M when connected to mellanox resulted in CRC errors.
Workaround:	Fixed with new preemphasis settings for DAC cables >=4m
PR# 162030	
Severity:	Sev 2
Synopsis:	TCP load balancing always remains in enabled state after the load-balance tcp-udp command is used.
Release Notes:	When the load-balance tcp-udp enable command is issued followed by the no load-balance tcp-udp command, the TCP load balancing mechanism does not revert to a disabled state.
Workaround:	
PR# 162046	
Severity:	Sev 2
Synopsis:	If the MTU size is changed after shutting down the interface, the OSPF network type moves back to the default, which causes the OSPF routes to fail.
Release Notes:	When the OSPF network type is set to P2P, if the MTU size is changed after shutting down the interface, the OSPF network type moves back to the default (broadcast), which causes the OSPF routes to fail.
Workaround:	Change the MTU size without shutting down the interface or reconfigure the network type after MTU change.
PR# 162086	
Severity:	Sev 2
Synopsis:	In a VLT setup, some DHCP packets are dropped as the VLT peers act as DHCP relay agents.
Release Notes:	When a DHCP discover message is received on one peer and the response is sent by the other peer through the VLTi, some DHCP packets are dropped.

Workaround: None.

PR# 162120

Severity: Sev 2

Synopsis: The system experiences a software exception during the Codenomicon OSPFv3 Test Suite 5.1.0.

Release Notes: The system experiences a software exception during the Codenomicon OSPFv3 Test Suite 5.1.0.

Workaround: None.

PR# 162121

Severity: Sev 2

Synopsis: BGP router-ID is not included in the startup and running configuration.

Release Notes: BGP router-ID is not included in the startup and running configuration.

Workaround: None.

PR# 162147

Severity: Sev 2

Synopsis: 802.1x authentication does not work on stack standby and member units.

Release Notes: 802.1x authentication does not work on stack standby and member units.

Workaround: None.

PR# 162197

Severity: Sev 2

Synopsis: In certain scenarios, DHCP does not work.

Release Notes: In certain scenarios, after booting up, DHCP does not work.

Workaround: Flap the L3 VLAN interfaces.

PR# 162257

Severity: Sev 2

Synopsis: Openflow action Groupmod fails, and returns a false error to the controller for the un-supported groupMod type, Fastfailover.

Release Notes: Openflow action Groupmod fails, and returns a false error to the controller for the un-supported groupMod type, Fastfailover.

Workaround: None.

PR# 162430

Severity:	Sev 1
Synopsis:	In certain scenarios, load balance settings do not persist after a failover or reload.
Release Notes:	In certain scenarios load balance settings do not persist after a failover or reload.
Workaround:	Use the load-balance command to reconfigure the switch.

PR# 162485

Severity:	Sev 2
Synopsis:	Modifying the MIB table dot1qVlanStaticTable does not work for interfaces configured as 'portmode hybrid'.
Release Notes:	Modifying the MIB table dot1qVlanStaticTable does not work for interfaces configured as 'portmode hybrid'.
Workaround:	None.

Fixed S4810 9.11(0.0) Software Issues

The following issues have been resolved in the Dell Networking OS version 9.11(0.0):

ARP (Resolved)

PR# 152155

Severity:	Sev 3
Synopsis:	BFD over static route fails to come up when a management route with subnet 0.0.0.0/0 is configured on the management interface.
Release Notes:	BFD over static route fails to come up when a management route with subnet 0.0.0.0/0 is configured on the management interface.
Workaround:	None.

BGP (Resolved)

PR# 160978

Severity:	Sev 1
Synopsis:	System reloads when same BGP route prefix is learned and aggregated through multiple neighbors.
Release Notes:	System reloads when same BGP route prefix is learned and aggregated through multiple neighbors.
Workaround:	None.

DHCP (Resolved)

PR# 160885

Severity:	Sev 2
Synopsis:	In BMP mode, DHCP request from the device does not include option 54.
Release Notes:	In BMP mode, DHCP request from the device does not include option 54.
Workaround:	None.

PR# 160890

Severity:	Sev 3
Synopsis:	Client do not get an IP address when dhcp snooping is enabled on a second router from the the dhcp client.
Release Notes:	Client do not get an IP address when dhcp snooping is enabled on a second router from the the dhcp client.
Workaround:	NA

FIB (Resolved)

PR# 159617

Severity:	Sev 2
Synopsis:	Communication between hosts connected to same numbered ports across stack units is not working
Release Notes:	Communication between hosts connected to same numbered ports across stack units is not working. For example, hosts connected to 0/1 may not be able to contact host connected to 2/1 in a stack setup and so on.
Workaround:	None

Fipsnooping (Resolved)

PR# 159302

Severity:	Sev 2
Synopsis:	The system loses FCOE sessions after the server reboots.
Release Notes:	In certain scenarios, due to a race condition, the established FCOE session gets lost after the server reboots.
Workaround:	Use the shutdown and no shutdown commands to restart the server interface.

FTSA (Resolved)

PR# 160967

Severity:	Sev 2
Synopsis:	SupportAssist does not work behind a proxy server.
Release Notes:	SupportAssist does not work behind a proxy server.
Workaround:	None.

IP Stack (Resolved)

PR# 160829

Severity:	Sev 2
Synopsis:	In certain scenarios, if the next hop for the management VRF route is reachable also through default VRF, then management route is not reachable.
Release Notes:	In certain scenarios, if the next hop for the management VRF route is reachable also through default VRF, then management route is not reachable. The issue is dependent on the order in which the management VRF is created.
Workaround:	Use interface name, that is "managementethernet" instead of the next-hop address in the route configuration.

Linecards (Resolved)

PR# 159427

Severity: Sev 1

Synopsis: When an untagged VLAN which is part of an ACL-vlan group is removed and reapplied as a member, traffic from tagged VLANs is dropped.

Release Notes: When an untagged VLAN which is part of an ACL-vlan group is removed and reapplied as a member, traffic from tagged VLANs is dropped. This issue happens when the same ports are members of tagged and untagged VLANs.

Workaround: Use the shutdown and no shutdown commands on the interfaces.

LLDP (Resolved)

PR# 158462

Severity: Sev 2

Synopsis: In rare scenarios, LLDP VLAN name TLV values are interpreted wrongly.

Release Notes: In rare scenarios, LLDP VLAN name TLV values are interpreted wrongly.

Workaround: None.

PR# 160705

Severity: Sev 3

Synopsis: LLDP fails when the management interface on the switch is assigned to the management VRF.

Release Notes: LLDP fails when the management interface on the switch is assigned to the management VRF. However, LLDP works without any issue when the management interface is assigned to the default VRF.

Workaround: None.

Microcode (Resolved)

PR# 150842

Severity: Sev 2

Synopsis: In certain scenarios, VRRP sessions flap when storm control is configured on the switch.

Release Notes: In certain scenarios, VRRP sessions flap when storm control is configured on the switch.

Workaround: None.

OS / OS Infrastructure (Resolved)

PR# 154390

Severity: Sev 1

Synopsis: Under certain circumstances, an SNMP request packet with the following OID causes the system to crash: 1.3.6.1.2.1.4.34.1.3.2.2.0x112.0xfe.

Release Notes: Under certain circumstances, an SNMP request packet with the following OID causes the system to crash: 1.3.6.1.2.1.4.34.1.3.2.2.0x112.0xfe.

Workaround: None.

PR# 158135

Severity:	Sev 2
Synopsis:	If a blank password is used to establish a telnet session over port 21, the system crashes.
Release Notes:	If a blank password is used to establish a telnet session over port 21, the system crashes.
Workaround:	None.

PR# 158812

Severity:	Sev 2
Synopsis:	Under certain scenarios, NLB Multicast traffic is not sent to the range of interfaces specified in the static MAC entry.
Release Notes:	Under certain scenarios, NLB Multicast traffic is not sent to the range of interfaces specified in the static MAC entry.
Workaround:	None.

PR# 159000

Severity:	Sev 2
Synopsis:	The system does not allow IPv6 addresses ending with 0 using /128 bit mask
Release Notes:	The system does not allow IPv6 addresses ending with 0 using /128 bit mask.
Workaround:	None.

PR# 159149

Severity:	Sev 1
Synopsis:	After upgrading to 9.9.0.0P9, the switch does not come up.
Release Notes:	After upgrading to 9.9.0.0P9 and rebooting, the switch does not come up due to corruption in the file system.
Workaround:	None.

PR# 159840

Severity:	Sev 3
Synopsis:	VLAN Name displays an extra space.
Release Notes:	VLAN Name displays an extra space.
Workaround:	None.

PR# 159893

Severity:	Sev 1
Synopsis:	The show processes cpu management-unit command displays incorrect details.
Release Notes:	The output of the CPUUtilization MIB get returns SYSDLP process CPU usage data instead of the system CPU usage data.

Workaround: None.

PR# 160431

Severity: Sev 3

Synopsis: In certain scenarios, the system displays unwanted error messages when it reloads.

Release Notes: In certain scenarios, the system displays unwanted error messages when it reloads.

Workaround: None.

PR# 160787

Severity: Sev 3

Synopsis: After upgrading to Dell Networking OS version 9.9(0.0) or later, the system may display EAPOL error messages.

Release Notes: After upgrading to Dell Networking OS version 9.9(0.0) or later, the system may display the following EAPOL error message if Dot1x is disabled in the previous version: EAPOL Frame MsgQ Send Err.

Workaround: None.

PR# 160879

Severity: Sev 1

Synopsis: Connecting to the switch frequently using telnet can cause the device to reboot.

Release Notes: The system may experience a software exception and reboot if connected through telnet or SSH very frequently.

Workaround: Decrease the frequency of telnet or SSH connections.

OSPF (Resolved)

PR# 156122

Severity: Sev 2

Synopsis: System chooses a static route with Administrative Distance (AD) greater than 110 over external OSPF routes.

Release Notes: System chooses a static route with Administrative Distance (AD) greater than 110 over external OSPF routes.

Workaround: None.

PR# 158232

Severity: Sev 1

Synopsis: In a VLT environment, routes leaked between VRFs are incorrectly learnt without taking Administrative Distance into account.

Release Notes: In a VLT environment, routes leaked between VRFs are incorrectly learnt without taking Administrative Distance into account.

Workaround: None.

PR# 160892

Severity:	Sev 2
Synopsis:	If the default-information-originate always command is configured, route loops may occur.
Release Notes:	In certain scenarios, if the default-information-originate always command is configured on OSPF neighbors, route loops can occur.
Workaround:	None.

PR# 161209

Severity:	Sev 2
Synopsis:	In certain scenarios, the system experiences a software exception on reboot when the max-metric router-lsa on-startup command is configured.
Release Notes:	The system experiences a software exception on reboot when max-metric router-lsa on-startup command is configured. This issue happens when the no passive-interface command is configured on an interface without an IP address.
Workaround:	Assign an IP address to the interface on which the no passive-interface command is configured.

PR# 161365

Severity:	Sev 2
Synopsis:	The system experiences a software exception during the OSPFv2 test of Codenomicon Defensics 11.11.0 test number 94307.
Release Notes:	The system experiences a software exception during the OSPFv2 test of Codenomicon Defensics 11.11.0 test number 94307. It tests the system's ability to handle LSU packet with zero LSA length and nonzero LSA count.
Workaround:	None.

Port Monitoring (Resolved)

PR# 158903

Severity:	Sev 3
Synopsis:	The show monitor session command does not display the session status.
Release Notes:	The show monitor session command has been enhanced to display whether the remote monitoring session is enabled or disabled in the system.
Workaround:	None.

SNMP (Resolved)

PR# 159437

Severity:	Sev 2
Synopsis:	The system displays an authentication error with SNMP v3.
Release Notes:	While using SNMP v3 Get request, the system displays an authentication error even if it is in the discovery phase and hence, it is not valid error condition.
Workaround:	None.

Spanning Tree (Resolved)

PR# 159697

Severity: Sev 1

Synopsis: When a large number of VLANs are configured using MSTP, the output of the show running-config command does not display all the configured VLANs.

Release Notes: When a large number of VLANs are configured using the msti vlan command, the output of the show running-config spanning-tree mstp command does not display all the configured VLANs.

Workaround: None.

Stacking (Resolved)

PR# 155356

Severity: Sev 3

Synopsis: The show hardware stackunit 0 stack-ports command incorrectly displays valid stack ports as invalid.

Release Notes: The show hardware stackunit 0 stack-ports command incorrectly displays valid stack ports as invalid.

Workaround: None.

Telnet (Resolved)

PR# 158792

Severity: Sev 2

Synopsis: In certain rare scenarios, the telnet process experiences a software exception.

Release Notes: In certain rare scenarios, the telnet process experiences a software exception. This does not affect user traffic.

Workaround: None.

PR# 161065

Severity: Sev 2

Synopsis: In BMP mode, the telnet server cannot be disabled.

Release Notes: The no ip telnet server enable command does not work in BMP mode.

Workaround: Use the following commands to disable the telnet server: 1. ip telnet server enable 2. no ip telnet server enable

VLT (Resolved)

PR# 158985

Severity: Sev 2

Synopsis: VLT does not function correctly when one peer runs Dell Networking OS version below 9.9(0.0) and the other runs version 9.9(0.0) or above.

Release Notes: When one VLT device is upgraded to Dell Networking OS version 9.9(0.0) or later from an earlier version, and the peer VLT device still runs a version less than 9.9(0.0), VLT does not function correctly for some features due to certain mismatch in the feature related VLT message exchanges. The affected features include: 1. PVST 2. VLT Q-in-Q 3. CLI batch 4. Provider bridge group Once the problem manifests, the behavior persists even after the peer VLT device is upgraded to the same version. It recovers only when both the VLT peers reboot simultaneously.

Workaround:	- Upgrade the VLT secondary switch and reboot. - Before VLT secondary switch comes up and establishes VLT, shutdown VLTi link on the primary device. - Upgrade the VLT primary and reboot. - Once the VLT primary device is up, use the no shutdown command to enable the VLTi link.
VRRP (Resolved)	
PR# 159635	
Severity:	Sev 2
Synopsis:	Using VRRP version 3 for IPv4 VRRP groups is not interoperable with other vendor routers
Release Notes:	This release fixes an issue that prevented interoperability of Dell OS9 routers with other vendor routers when using VRRP version 3 for IPv4 VRRP groups. Typically VRRPv2 is used for IPv4 VRRP groups and VRRPv3 for IPv6 groups. Those have always been interoperable. With this fix, using VRRPv3 for IPv4 VRRP groups will be interoperable as well.
Workaround:	When interoperating with other vendor routers use VRRP version 2 for all IPv4 VRRP groups.

Known Issues

Known issues are reported using the following definitions.

Category	Description
PR#	Problem Report number that identifies the issue.
Severity	**S1** — Crash: A software crash occurs in the kernel or a running process that requires a restart of AFM, the router, switch, or process. **S2** — Critical: An issue that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no work-around acceptable to the customer. **S3** — Major: An issue that affects the functionality of a major feature or negatively effects the network for which there exists a work-around that is acceptable to the customer. **S4** — Minor: A cosmetic issue or an issue in a minor feature with little or no network impact for which there might be a work-around.
Synopsis	Synopsis is the title or short description of the issue.
Release Notes	Release Notes description contains more detailed information about the issue.
Work around	Work around describes a mechanism for circumventing, avoiding, or recovering from the issue. It might not be a permanent solution. Issues listed in the “Closed Caveats” section should not be present, and the work-around is unnecessary, as the version of code for which this release note is documented has resolved the caveat.

Known S4810 Software Issues

The latest information related to Open Caveats is available on iSupport through the BugTrack search tool. BugTrack currently tracks software caveats opened in Dell Networking OS version 6.2.1.1 and later.

NOTE: You must have a user account to access the BugTrack tool.

To use the search tool:

1 Go the Main Customer Support page: https://www.force10networks.com/csportal20/Main/SupportMain.aspx.
2 Log in.
3 Click the BugTrack link, located in the Quick Links menu directly below the login bar.
This takes you to the BugTrack search page: https://www.force10networks.com/csportal20/BugTrack/SearchIssues.aspx.
4 Enter for a specific PR or select an Dell Networking OS version, platform, Severity, or category to get a list of PRs.
5 Click the Search button.
6 Click the PR number to view specific PR details.

The PR (or PRs) appears on the page below the tool.

The following caveats are open in Dell Networking OS version 9.11(0.0):

ARP (Open)

PR# 141762

Severity:	Sev 2
Synopsis:	In some instance, when the link status of VLT ICL flap, the show ip redirect list command may incorrectly show the unresolved next-hops as resolved.
Release Notes:	In some instance, when the link status of VLT ICL flap, the show ip redirect list command may incorrectly show the unresolved next-hops as resolved.
Workaround:	To display the correct ARP resolve status, re-configure the PBR redirect list after deleting it.

BGP (Open)

PR# 159068

Severity:	Sev 3
Synopsis:	The neighbor update-source BGP command supports all Layer 3 interfaces.
Release Notes:	The neighbor update-source BGP command supports all Layer 3 interfaces.
Workaround:	None.

DCB (Open)

PR# 107320

Severity:	Sev 3
Synopsis:	ETS on PFC enabled PGID's may not confirm to the configuration, when port-mirroring is enabled and corresponding packets are mirrored.
Release Notes:	ETS on PFC enabled PGID's may not confirm to the configuration, when port-mirroring is enabled and corresponding packets are mirrored.
Workaround:	No workaround.

PR# 108226

Severity:	Sev 3
Synopsis:	In DCBx-CIN version, priorities belonging to 'Strict priority priority-group' are incorrectly listed as ETS type in the 'show ets detail' output

Release Notes:	Though priorities are associated to a 'Strict priority priority-group' in a dcb-output profile that is applied to an interface,they are incorrectly listed as ETS type in the priority-level bandwidth splitup that is displayed in the 'show ets detail' output when the interface has dcbx version to be CIN
Workaround:	This is just a display issue and doesn't affect the functionality in any way

FIB (Open)

PR# 138294

Severity:	Sev 2
Synopsis:	The maximum number of supported Microsoft NLB cluster IPs is increased from 8 to 11
Release Notes:	The maximum number of supported Microsoft NLB cluster IPs is increased from 8 to 11
Workaround:	None

IP Stack (Open)

PR# 160864

Severity:	Sev 2
Synopsis:	In certain scenarios, IPv6 processing may take a long time causing high CPU usage.
Release Notes:	A software exception causes the IPv6 processing to take a long time. This behavior results in high CPU usage and the switch may reboot.
Workaround:	None.

PR# 160891

Severity:	Sev 2
Synopsis:	The system may experience a software exception if an interface receives router advertisements with multiple IPv6 prefixes.
Release Notes:	The system may experience a software exception if an interface receives router advertisements with multiple IPv6 prefixes.
Workaround:	None.

PR# 161131

Severity:	Sev 2
Synopsis:	Management VRF route not working if NH reachable via unicast routing table
Release Notes:	Management VRF route not working if NH reachable via unicast routing table
Workaround:	Use interface-name (ie. management) instead of next-hop address in the route configuration. --> management route 0.0.0.0/0 managementethernet (instead of) management route 0.0.0.0/0 10.10.238.169

PR# 161297

Severity:	Sev 2
Synopsis:	Router advertisement (RA) flooding on a layer 3 IPv6 interface causes the system to reboot.
Release Notes:	The system experiences a software exception when a layer 3 IPv6 interface is flooded with too many router advertisements.

Workaround:	None.
PR# 161469	
Severity:	Sev 2
Synopsis:	IPV6 VLT convergence time is more than 2 seconds during ICL no shut/ primary node reboot
Release Notes:	When STP/PVSTP is enabled and ICL is flapped, STP detects topology change. This topology change event will flush ND entries. ND entries has to be relearned for data traffic to resume.
Workaround:	None. Traffic loss is seen during the interval of deleting and relearning ND entries. Also issue will be happen only with STP/PVSTP enabled
Layer 2 (Open)	
PR# 152033	
Severity:	Sev 3
Synopsis:	In Dell Networking OS release 9.9(0.0), VLT mismatch occurs with the default VLAN ID (VLAN ID 1) when VLT is activated.
Release Notes:	In Dell Networking OS release 9.9(0.0), VLT mismatch occurs with the default VLAN ID (VLAN ID 1) when VLT is activated.
Workaround:	Change the default VLAN ID to anything other than 1.
Layer 3 (Open)	
PR# 126181	
Severity:	Sev 3
Synopsis:	IPv6 address configured on a shutdown interface may be advertised to neighboring devices via routing protocols.
Release Notes:	IPv6 address configured on a shutdown interface may be advertised to neighboring devices via routing protocols.
Workaround:	Remove and reapply " ipv6 ospf area " to stop advertisement of IPv6 address configured on shutdown interface
LLDP (Open)	
PR# 118185	
Severity:	Sev 3
Synopsis:	Tab completion doesn't work for the last keyword in "advertise management-tlv" command.
Release Notes:	Tab completion doesn't work for the last keyword in "advertise management-tlv" command.
Workaround:	NA
Multicast (Open)	
PR# 118195	
Severity:	Sev 3
Synopsis:	After PIM DR change on a VLT node, multicast data traffic may not reach receivers in some VLANs
Release Notes:	On a VLT pair, when a PIM DR undergoes a change of status, receivers in some VLANs stop receiving multicast traffic.
Workaround:	clear the pim data base by issueing command "clear pim tib".

PR# 147768

Severity:	Sev 2
Synopsis:	If IGMP receiver connected to VLT LAG makes a silent leave, VLT LAG is not removed from the member port list in IGMP Snooping table
Release Notes:	If IGMP receiver connected to VLT LAG makes a silent leave for a group, the VLT LAG would not be removed from the member port list of IGMP snooping table. This could happen when the VLAN interface having the VLT LAG is running IGMP version 2. Multicast data traffic would continue to flow to the VLT LAG.
Workaround:	Configure IGMP version 3 on the VLAN having the receivers. This problem would not be seen if the VLAN interface is running version 3 and having version2/version3 receivers. (or) Execute clear ip igmp snooping groups to clear out the stale entry

PR# 155900

Severity:	Sev 2
Synopsis:	In certain scenarios, the static multicast mac address command exceeds the maximum characters (256) that can be entered at the command prompt.
Release Notes:	In certain scenarios, the static multicast mac address command exceeds the maximum characters (256) that can be entered at the command prompt. This limitation causes less number of interfaces to be configured.
Workaround:	None.

OS / OS Infrastructure (Open)

PR# 108305

Severity:	Sev 3
Synopsis:	NTP server configured with hostname is not updating the IP change for server
Release Notes:	NTP server configured with hostname is not updating the IP change for server
Workaround:	Unconfigure and reconfigure the NTP server and it resolves to the new IP.

OSPF (Open)

PR# 149808

Severity:	Sev 3
Synopsis:	When the VLAN MTU changes on the peer router, the corresponding OSPF session goes down.
Release Notes:	When the VLAN MTU changes on the peer router, the corresponding OSPF session goes down.
Workaround:	None.

QoS (Open)

PR# 159890

Severity:	Sev 2
Synopsis:	If first match criteria of a match-any class map is an L3 acl, and if it's not a match, traffic matching the other criteria are not honoring the policy

Release Notes:	In a class map created with a match-any option, the "any" does not take effect, if the first match criteria is a different L3 ACL created using "ip access-list" instead of an explicit rule. Policy takes effect only if the first match criteria is satisfied.
Workaround:	While using match-any option in a class-map, use explicit rules instead of using an ACL created using "ip access-list".

Spanning Tree (Open)

PR# 123322

Severity:	Sev 2
Synopsis:	PVST fails to converge between Dell-Force10 and other vendor devices on non-default native VLAN.
Release Notes:	PVST fails to converge between Dell-Force10 and other vendor devices on non-default native VLAN. This issue occurs only when the native vlan is non-default (other than VLAN-1).
Workaround:	Use default vlan-1 as native VLAN when interop with other vendor device. Another workaround is to configure Dell-Force10 switch with higher priority value so that it won't become the root.

PR# 151669

Severity:	Sev 2
Synopsis:	The port-channel interfaces that are activated after the lacp ungroup member-independent vlt command is configured may cause traffic drops.
Release Notes:	The port-channel interfaces that are activated after the lacp ungroup member-independent vlt command is configured may cause traffic drops.
Workaround:	None.

SSH (Open)

PR# 160683

Severity:	Sev 1
Synopsis:	SSH Server Terminates Connection with BAD Termination Status
Release Notes:	SSH Server Terminates Connection with BAD Termination Status
Workaround:	None.

Support Resources

The following support resources are available for the S4810 system.

Documentation Resources

This document contains operational information specific to the S4810 system.

For information about using the S4810, refer to the following documents at http://www.dell.com/support:

- *Installing the S4810 System*
- *Quick Start Guide*
- *Dell Networking Command Line Reference Guide for the S4810 System*

- *Dell Networking Configuration Guide for the S4810 System*

For more information about hardware features and capabilities, refer to the Dell Networking website at https://www.dell.com/networking.

For more information about the open network installation environment (ONIE)-compatible third-party operating system, refer to http://onie.org.

Issues

Issues are unexpected or incorrect behavior and are listed in order of Problem Report (PR) number within the appropriate sections.

NOTE: You can subscribe to issue update reports or use the BugTrack search tool to read current information about open and closed issues. To subscribe or use BugTrack, visit Dell Support at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx.

Finding Documentation

This document contains operational information specific to the S4810 system.

- For information about using the S4810, refer to the documents at http://www.dell.com/support.
- For more information about hardware features and capabilities, refer to the Dell Networking website at https://www.dell.com/networking.
- For more information about the open network installation environment (ONIE)-compatible third-party operating system, refer to http://onie.org.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

Go to www.dell.com/support.