Dell™ PowerConnect™
8132/8164/8132F/8164F/7024/7048/7024P/7048P/7024F/7048R/
7048R-RA/8024/8024F/M6220/M6348/M8024/M8024-k

PowerConnect 5.1.0.1 Firmware Release Notes

Date: April 2013
System Firmware Version 5.1.0.1

Table of Contents

PowerConnect 8132/8164/8132F/8164F/8024/8024F/M8024/M8024-k/ M6220/M6348/7024/7048/7024P/7048P/7024F/7048R/7048R-RA Release Notes

Introduction

This document provides specific information for the Dell PowerConnect 8132/8164/8132F/8164F/7024/7048/7024P/7048P/7024F/7048R/7048R-RA/8024/8024F/M6220/M6348/M8024/M8024-k switches firmware version 5.1.0.1.

It is recommended that this release note be thoroughly reviewed prior to installing or upgrading of this product.

Global Support

For information regarding the latest available firmware, release note revisions, or additional assistance, please visit support.dell.com.

Firmware Specifications

Firmware Version

Firmware Image Name	Version Number	Release Date
PC8100v5.1.0.1.stk	**5.1.0.1**	**April 2013**
PCM6220v5.1.0.1.stk	**5.1.0.1**	**April 2013**
PC7000_M6348v5.1.0.1.stk	**5.1.0.1**	**April 2013**
PC8024v5.1.0.1.stk	**5.1.0.1**	**April 2013**
PCM8024v5.1.0.1.stk	**5.1.0.1**	**April 2013**
PCM8024kv5.1.0.1.stk	**5.1.0.1**	**April 2013**

Version Numbering Convention					
Version number					**Description**
PowerConnect Series	5	1	0	1	Four part version number
				t	Denotes the build number.
			t		Denotes an ad hoc release of the product software.
		t			Denotes a scheduled maintenance release of the product software.
	t				Denotes a major version number.

Firmware Upgrade

NOTE: Administrators upgrading PowerConnect 7024/7048/7024P/7048P/7024F/7048R/7048R-RA/8024/8024F/M6220/M6348/M8024/M8024k switches from 2.x.x.x or 3.x.x.x or 4.x.x.x or 5.0.x.x versions of firmware MUST follow the instructions documented in the **Upgrading PowerConnect Switches from Version 2.x.x.x or 3.x.x.x or 4.x.x.x or 5.0.x.x to 5.1.0.1 Firmware** procedure. Failure to follow the procedures described in that document when upgrading from 2.x.x.x or 3.x.x.x or 4.x.x.x or 5.0.x.x firmware may result in an inoperable switch!

NOTE: After upgrading the switch firmware version to 5.1.0.1, the CPLD (Complex Programmable Logic Device) code update is required on M8024-k and PC8024/PC8024F switches via serial console if switch is running with the older CPLD version. The latest CPLD version available for M8024k switch is Version 5 and for PC8024/PC8024F switch is Version 6. Administrators upgrading PowerConnect 8024/8024F/M8024k switches MUST follow the CPLD update instructions documented in the **Upgrading PowerConnect Switches from Version 2.x.x.x or 3.x.x.x or 4.x.x.x or 5.0.x.x to 5.1.0.1 Firmware** procedure.

NOTE: Administrators upgrading PowerConnect 8132/8164/8132F/8164F switches MUST follow the instructions documented in the **Upgrading PowerConnect 8132_8164_8132F_8164F switches from Version 5.0.x.x to 5.1.0.1 Firmware** procedure. Failure to follow the procedures described in that document when upgrading firmware may result in an inoperable switch!

NOTE: OMNM (Open Manage Network Manager) v5.2 SP1 supports firmware management of PowerConnect 7024/7048/7024P/7048P/7024F/7048R/7048R-RA/8024/8024F/M6220/M6348/M8024/M8024-k to deploy the firmware version 4.1.x.x or later. OMNM v5.2 SP1 supports PowerConnect 8132/8164/8132F/8164F to deploy the firmware version 5.0.0.4

Firmware Downgrade

Downgrading from 5.1.0.1 to an earlier release is supported on most PowerConnect series switches (except PC81xx series with B1 CPU versions, see note below); however, migration of configuration information from a later release to an earlier release is not supported. The existing configuration may or may not work with the earlier version of firmware, therefore, it is best to be physically present at the switch site and to be prepared to access the switch over the serial port if necessary when downgrading firmware.

Auto-downgrade of a stack is not enabled by default. If downgrading a stack, be sure to enable auto-downgrade before activating the earlier versions of firmware on the stack master.

Recent versions of the PowerConnect 81xx series switches support newer versions of CPU (B1). The B1 version of CPU requires Release 5.1.0.1 or later firmware and cannot be downgraded to earlier releases. In addition, if this unit is to be deployed as a member within a stack, the entire stack will be required to run 5.1.0.1 or later firmware. Here are some steps to help determine what CPU is in the PowerConnect 8100 Series switch:

1. Run **show version** from the CLI prompt.
2. If there is no CPU version line, then the stack is running 5.0.x.x firmware. Since 5.0.x.x can only run on A1 CPU switches, then all switches in the stack (or a standalone) contain A1 CPUs.
3. If there is a CPU version line (like below):
   CPU Version..... XLP308H-A1
   (It will display the CPU version in the last two characters - either A1 or B1).
4. On a stack, run **show version *m*** where *m* is the unit number assigned to the stack member to see each CPU version for each member in the stack.

In addition here are the part numbers for reference:

Part Numbers for PowerConnect 81xx	A1 CPU	B1 CPU
PowerConnect 8132 (US, Canada, Mexico, South America)	TRJ78	PTM0F
PowerConnect 8132 (all other countries)	0C90P	X20W5
PowerConnect 8132F (US, Canada, Mexico, South America)	W0HV1	NWHGV
PowerConnect 8132F (all other countries)	7D1GN	KWHG3
PowerConnect 8164 (US, Canada, Mexico, South America)	H0F6C	N00C1
PowerConnect 8164 (all other countries)	P8RHX	Y2FJ0
PowerConnect 8164F (US, Canada, Mexico, South America)	VTWN8	4PHP2
PowerConnect 8164F (all other countries)	1JWM5	8KHT1

Recent versions of the PowerConnect M8024-K modular switches have hardware changes that require firmware version 4.1.0.19 or higher. PowerConnect M8024-K with a new PPID label cannot be downgraded below 4.1.0.19. If a downgrade is attempted, the firmware activation procedure will detect that earlier firmware is not compatible with the switch hardware and abort the activation procedure. Any PowerConnect M8024-K with the old PPID label can accept any version of the switch firmware.

MODEL	OLD PPID	NEW PPID
M8024K	2F07F A00	2F07F A01
	57821 A00	57821 A01

Boot Code Downgrade

Never downgrade the boot code! The 5.1.0.1 boot code supports all earlier versions of firmware and never needs downgrading.

Hardware Supported

- Dell PowerConnect 8132 Ethernet Switch
- Dell PowerConnect 8164 Ethernet Switch
- Dell PowerConnect 8132F Ethernet Switch
- Dell PowerConnect 8164F Ethernet Switch
- Dell PowerConnect M6220 Ethernet Switch
- Dell PowerConnect M6348 Ethernet Switch
- Dell PowerConnect 7024 Ethernet Switch
- Dell PowerConnect 7048 Ethernet Switch
- Dell PowerConnect 7024P Ethernet Switch
- Dell PowerConnect 7048P Ethernet Switch
- Dell PowerConnect 7024F Ethernet Switch
- Dell PowerConnect 7048R Ethernet Switch
- Dell PowerConnect 7048R-RA Ethernet Switch
- Dell PowerConnect 8024 Ethernet Switch
- Dell PowerConnect 8024F Ethernet Switch
- Dell PowerConnect M8024 Ethernet Switch
- Dell PowerConnect M8024-k Ethernet Switch

Support Matrix

Since not all functionality is supported on all switches, the following matrix identifies the major differences among the PowerConnect switch models. A check mark indicates support for the feature. All other features listed in the release notes are supported on all switches.

Feature/Switch	Priority Flow Control	DCBx	ETS	PoE+	iSCSI Optimization	USB	grEEEn Ethernet	Hot Swap Cards	WRED
Dell PowerConnect M6220 Ethernet Switch									
Dell PowerConnect M6348 Ethernet Switch					✓				✓
Dell PowerConnect 7024 Ethernet Switch					✓	✓	✓	✓	✓
Dell PowerConnect 7048 Ethernet Switch					✓	✓	✓	✓	✓
Dell PowerConnect 7024P Ethernet Switch				✓	✓	✓	✓	✓	✓
Dell PowerConnect 7048P Ethernet Switch				✓	✓	✓	✓	✓	✓
Dell PowerConnect 7024F Ethernet Switch					✓	✓	✓	✓	✓
Dell PowerConnect 7048R Ethernet Switch					✓	✓	✓	✓	✓
Dell PowerConnect 7048R-RA Ethernet Switch					✓	✓	✓	✓	✓
Dell PowerConnect 8024 Ethernet Switch	✓	✓			✓				✓
Dell PowerConnect 8024F Ethernet Switch	✓	✓			✓				✓
Dell PowerConnect M8024 Ethernet Switch					✓				✓
Dell PowerConnect M8024-k Ethernet Switch	✓	✓			✓				✓
Dell PowerConnect 8132 Ethernet Switch	✓	✓	✓		✓	✓	✓	✓	✓
Dell PowerConnect 8164 Ethernet Switch	✓	✓	✓		✓	✓	✓	✓	✓
Dell PowerConnect 8132F/8164F Ethernet Switch	✓	✓	✓		✓	✓	✓	✓	✓

Supported Firmware Functionality

For more details regarding all the supported firmware features and functionality, please refer to the Dell PowerConnect Series CLI Reference Guide and the Dell PowerConnect Series User's Configuration Guide.

Added Functionality in this Release

This section contains a list of features added in this release that are new for at least one switch listed in the **Hardware Supported** section above.

Release 5.1.0.1

- IGMP Snooping Improvements
- IP Multicast Enhancements
- Support for B1 CPU – only on PC8100 series
- New Browser Support
  - Mozilla Firefox 14
  - Internet Explorer 9
  - Google Chrome 21
- Static Route Maximum Increased to 512 (for all switches except for M6220 series)
- USB Auto-configuration expanded for multiple MAC Address support
- Ability to reset stack port counters
- Increased Maximum number of dot1x clients per port to 24
- Commands to remove signed certificates/Keys
- Support for Additional transceivers/optics

Release 5.0.1.3

- Added PoE DC Disconnect HW support – on PC7000 series

Release 5.0.0.4

- Added Native EEE Support for the PC8100 10GBaseT Ports
- 802.1Qaz (ETS) – on 8100 series
- Support for 40 Gig (QSFP+) interfaces
- Support for Bootcode upgrade from pre-4.x image to 5.x image without manual system reset.
- Local Preference for LAG
- Private VLAN
- CLI output filtering
- Routing Improvements for OSPF
- UDLD
- Administrative Profiles
- AAA Authorization
- TACACS+ Accounting
- Stacking over QSFP+ ports
- QSFP+ diagnostics
- sFlow Support on Port Channels

Release 4.2.2.3

- No Added Functionality in this Release

Release 4.2.1.3

- No Added Functionality in this Release

Release 4.2.0.4

- DCBx on M8024-k/8024/8024F
- FIP Snooping Bridge on M8024-k/8024/8024F
- Add EEE Support for the PC7000 10GBaseT Ports
- GUI EEE Power Savings Charts
- RP Failover Performance Improvement
- Flexible Dynamic LAG Limits
- CLI Help Usability Improvements
- Ability to Show Static Route Entries
- CMC XML Support
- Stacking Over Ethernet Ports
- Change Dell EqualLogic iSCSI Auto Detect to default
- Add CLI Macro (Port Profile) for Dell Compellent Storage Equipment
- Provide Dell EqualLogic DCBx TLV Auto Detect and Configuration on M8024-k/8024/8024F

Release 4.1.1.9

- No Added Functionality in this Release

Release 4.1.0.19

- Media-type CLI command

  Added new command "media-type" to configure an interface to select the specified media on a combo port. It is recommended the administrators select the specific media type for the particular type of network connection they expect to use. Users may observe a single port flap when the media type is changed from RJ45 to auto-select RJ45 and only the corresponding SFP port is enabled. Refer to the CLI Reference Guide Updates section below for the complete syntax.

Release 4.1.0.6

- IPv4-Only Mode Optimization

  PowerConnect switches allocate the maximum sizes for routing tables (and others, as applicable) for both IPv4 and IPv6. Switch Performance Optimization allows the operator to optimize the allocation of switch silicon tables for either IPv4 only or mixed IPv4/IPv6 operation. The template specified limits are enforced by routing components when routes are being learned. When IPv4 only mode is selected, the following capabilities are disabled:

  - DHCPv6 relay
  - DHCPv6 server
  - IPv6 routing/forwarding
  - OSPFv3
  - IPv6 Neighbor Discovery
  - Configured v6-over-v4 tunnels
  - Automatic (6to4) tunnels
  - IPv6 Multicast

  A reboot is required when changing to or from IPv4 mode.

- Auto-Install

  USB based auto-install is an easy way to quickly bring up a switch with a known configuration. Network based auto-install is useful in rolling out a configuration or firmware update to a group of switches or in maintaining a central repository of switch configurations and firmware where the switches always obtain their firmware and configuration from a central server.

  The following clarifications are helpful in understanding the processing steps in auto-install:

  - Always power on the switch that is desired to be the stack master first
  - Auto-install never proceeds if a startup-config file is present on the (master) switch
  - USB auto-install is attempted first. Network auto-install only proceeds if USB auto-install fails.
  - If there are multiple .setup files present on the USB flash device, the powerconnect.setup file is selected
  - If a valid .setup file is not found on the USB flash device, the single .text file is used
  - If multiple .text files are present, the powerconnect.text file is used.

  Network based auto-install utilizes information obtained from a DHCP server. Refer to the documentation for a discussion of the DHCP options used by Auto-Install.

  When auto-install downloads a firmware image to switch memory, it compares the version to the current switch image. If different, the image in memory is copied to the switch backup image and activation of the image is attempted. If activation succeeds, the switch is rebooted and auto-install then attempts configuration file download.

  Auto-install configuration files are executed as a script. For more details on Auto-Install, refer to the User's Guide.

- Link Local Protocol Filtering

  Link Local Protocol Filtering blocks Cisco link local protocols from being flooded in the network. By default, PowerConnect switches process and respond to Cisco CDP packets. However, in networks where this capability is not desirable or other Cisco proprietary packets are flooded over the network, the administrator can disable flooding of Cisco link local protocols. The following table identifies the matching criteria for filtering Cisco proprietary packets:

Rule Type	Rule Purpose	Blocked Destination MAC Address	Ether Type
Blockcdp	Used to block CDP PDU's	N/A	0x2000
Blockvtp	Used to block VTP PDU;s	N/A	0x2003
Blockdtp	Used to block DTP PDU's	N/A	0x2004
Blockudld	Used to block UDLD PDU's	N/A	0x0111
Blockpagp	Used to block PAGP PDU's	N/A	0x0104
Blocksstp	Used to block SSTP PDU's	N/A	0x010b
Blockall	Used to block all defined Protocol Filtering PDU's	01:00.0C:CC:CC:C0	N/A

- DHCP Server

  The PowerConnect Series switches support a simple DHCP server capability for domains that do not wish to deploy a redundant DHCP address assignment solution or who have need of a temporary solution while (re)deploying their DHCP server solution.

In configuring DHCP scopes, be aware that the DHCP pool address and netmask must exactly match a VLAN address and netmask assignment for DHCP addresses to be served over that VLAN.

Only a single manual IP address can be assigned to a pool. The address must have a netmask of 32.

- GMRP

  The GARP Multicast Registration Protocol provides a mechanism that allows networking devices to dynamically register (and de-register) Group membership information with the MAC networking devices attached to the same segment, and for that information to be disseminated across all networking devices in the bridged LAN that support Extended Filtering Services. The PowerConnect Series switches support GMRP as specified in IEEE 802.1Q 1998.

- WRED

  Weighted Random Early Drop is supported on certain PowerConnect series switches. Refer to the table at the beginning of this section for further information. CoS queue configuration involves the following hardware port queue configuration parameters:

  - scheduler type: strict vs. weighted
  - minimum guaranteed bandwidth
  - maximum allowed bandwidth (i.e. shaping)
  - queue management type: tail drop vs. WRED
  - tail drop parameters: threshold
  - WRED parameters: minimum threshold, maximum threshold, drop probability

  Tail drop and WRED parameters are specified individually for each supported drop precedence level.
  In addition, the following are specified on a per-interface basis:
  - queue management type: tail drop vs. WRED (only if per-queue configuration is not supported)
  - WRED decay exponent

  Switch administrators should remember to configure ingress ports as trusted or un-trusted. By default ingress ports trust dot1p values.

- Stack Firmware Synchronization

  Stack firmware synchronization updates all stack members to the active firmware version on the master switch. Stack firmware synchronization is enabled by default. Stack firmware downgrade is enabled by default.

- Multicast VLAN Registration

  Multicast VLAN Registration provides a method of coalescing multicast traffic requested by users on multiple VLANs onto a single VLAN when carried over the network.

  MVR does not require that either source or receiver ports utilize VLAN tagging.

  Network planners are reminded that multicast groups in the 224.0.0.x range are reserved for multicast control plane traffic. Network planners should select multicast groups in another range for normal multicast traffic, e.g. 239.0.1.x

- iSCSI Optimization

  iSCSI Optimization automatically configures ports for use with the iSCSI protocol and tracks iSCSI sessions on the PowerConnect 7000 and 8000 Series switches as well as the PCM6348. Dell EqualLogic arrays are automatically detected and configuration of Dell EqualLogic connected ports is performed automatically.

  Administrators are advised that the configuration performed by enabling iSCSI optimization is not automatically reversed on disabling the feature. The administrator will need to manually remove the configuration settings when migrating Dell EqualLogic servers or iSCSI initiator ports to other ports or switches.

  Detection of Dell EqualLogic arrays is keyed on receipt of the mandatory System Description TLV in the LLDP packet. Disabling LLDP will effectively disable Dell EqualLogic array detection.

Dell EqualLogic arrays are required to be upgraded to firmware 5.0.2 or later in order to use the iSCSI Optimization feature.

- LLDP

  Administrators should ensure that LLDP-MED is enabled in order to operate EEE. Disabling LLDP or LLDP-MED will effectively disable EEE, IEEE 802.3at PoE+ high power negotiation and Dell EqualLogic array detection in the iSCSI Optimization feature.

- Connectivity Fault Management

  Connectivity Fault Management performs Metro Ethernet maintenance functions. Dell PowerConnect CFM supports the following functions defined in IEEE 802.1ag Draft 8.1:

  - Path discovery (link trace messages)
  - Fault detection (continuity check message)
  - Fault verification and isolation (loopback and link trace messages)
  - Fault notification (alarm indication signal or SNMP trap).

- Management IP Address Conflict Detection

  Management IP address conflict detection actively looks for duplicate IP address assignment and logs conflicts. Only the last identified IPv4 address conflict is retained for display by a show command. Administrators may examine the in- memory logs or the output from a SYSLOG server to identify the historical IP address conflicts. If console logging is enabled for traps, a message will appear on the console indicating that an address conflict has occurred.

- Email Alerting

  Email alerting allows administrators to be notified via email regarding system events. Multiple email addresses can be configured. The system will attempt to resolve mail servers specified with a FQDN immediately and, if successful, store the mail-server as an IP address. If a new IP address is subsequently assigned to the mail server, the operator will need to re-assign the email address on the switch.

  Only the Mail User Agent functionality of RFC 4409 is implemented. The PowerConnect switch does not implement SMTP server functionality.

- 802.1X Monitor Mode

  Monitor mode is a special debug mode that assists network administrators in configuring 802.1X authenticators. Users attempting to authenticate using the authenticator are always granted access when monitor mode is enabled. All interactions with the supplicant and the authentication server are logged.

  Administrators are cautioned against enabling monitor mode in a deployed network where 802.1X users may gain access to sensitive network resources.

- Time Controlled ACLs

  Time controlled ACLs allow administrators to apply ACLs based on the time of day. Both periodic and absolute time periods may be configured.

  Administrators are cautioned that invalid (overlapping) periodic entries within a time range will prevent the time range from being applied. Administrators are advised to test their periodic entries and validate that they become active as expected before deploying the time ranges in a production network. Administrators can check if a time range is active by using the *show time-range* command.

  It is recommended to enable ACL logging to ensure notice of ACL activation and de-activation.

- SNTP over IPv6

  SNTP operates over IPv4 and IPv6 and may be configured using IPv4 or IPv6 addresses or DNS.

- Strong Passwords

  The strong passwords feature allows administrators to specify that local switch passwords meet certain characteristics considered to enhance network security.

  Administrators are advised that the minimum character classes configuration must be enabled (value equal to 1 or greater) along with enabling the strong password feature before the other minimum character class configurations are enforced. These character class configurations are:

  - Minimum number of uppercase letters.
  - Minimum number of lowercase letters.
  - Minimum number of numeric characters.
  - Minimum number of special characters

  The password strength restrictions do not apply to users configured for the internal authentication server.

- Switch Auditing

  Switch auditing enhances network security by logging sensitive administrative actions. Switch auditing logs the following actions:

  - Successful login
  - Unsuccessful attempt to login
  - Logout out from the switch
  - Timed out logout from the switch
  - Download file to the switch
  - Upload file from the switch
  - Remove file from the flash
  - File changes on the flash
  - Clear configuration
  - Add or remove user
  - Change user access level

  Use of a SYSLOG server for monitoring network events is highly recommended.

- Authentication

  The PowerConnect switches support authentication via a number of methods. The methods are specified in named lists. Lists may be assigned to the enable and login access methods. The supported authentication methods are:

  - Enable
  - Line
  - RADIUS
  - TACACS
  - IAS
  - Local
  - None

  Methods are attempted in the order specified in the authentication list. If the authentication method rejects authentication, the user login is rejected. If an authentication method fails, e.g. unable to contact the authentication server, the next method in the list is attempted. The IAS, local and none methods can never fail so, if specified, must be last in the list.

  The 802.1X authentication list cannot be named and only supports the RADIUS, IAS, or none authentication methods. The 802.1X authentication can only have a single method.

- Internal Authentication Server

  The PowerConnect Series switches support 802.1X authentication of network users from an internal authentication database. IAS users are given access to network resources. IAS is not a valid method for login or enable authentication.

The IAS database can be downloaded to the switch using the "ias-users" target in the copy command. The ias-users file takes the form of a configuration script, as follows:

```
configure
aaa ias-user username client-1
password my-password1
exit
aaa ias-user username client-2
password aa5c6c251fe374d5e306c62496c3bcf6 encrypted
exit
aaa ias-user username 1f3ccb1157
password 1f3ccb1157
exit
```

IAS users may also be configured via the web interface.

- DNS Client

The PowerConnect Series switches support name resolution via an embedded DNS client. When a DNS name is specified, it is attempted to be resolved against the configured DNS servers immediately. The PowerConnect switches will store the resolved IP address. If the IP address of the host resolved via DNS changes, the administrator will need to update the configured IP address, either via DNS or manually.

If the switch is configured to obtain an address via DHCP, DNS server information received from the DHCP server is used to populate the DNS client configuration.

- Port Profiles (CLI Macros)

The PowerConnect series of switches provides a convenient way to save and share common configurations through the use of CLI macros. A CLI macro is a set of commands having a unique name. When a CLI macro is applied, the CLI commands contained within the macro are executed and added to the running configuration. When the macro is applied to an interface, the existing interface configurations are not lost; the new commands are added to the interface and are saved in the running configuration.

A CLI macro may have keywords (variables) which are replaced by values provided when the macro is applied (up to 3 keywords per macro). Macros can be applied to specific interfaces, a range of interfaces, or the global configuration.

Administrators may add their own macros or utilize the built-in macros.

Administrators are cautioned to ensure that a macro does not change command modes (e.g., change from interface configuration mode to global configuration mode).

The software includes 6 built-in macros:

- profile-global - the global configuration used to enable RSTP and loop guard.
- profile-desktop - the interface configuration for increased network security and reliability when connecting a desktop device, such as a PC, to a switch port.
- profile-phone - the interface configuration used when connecting a desktop device such as a PC with an IP phone to a switch port.
- profile-switch - the interface configuration used when connecting an access switch and a distribution switch or between access switches.
- profile-router - the interface configuration used when connecting the switch and a WAN router.
- profile-wireless- the interface configuration used when connecting the switch and a wireless access point.

Built-in macros may not be deleted or altered by the operator.

Changed Functionality in this Release

This section contains commentary on significant differences from previous releases of firmware on PowerConnect switches, e.g. the 8132/8164/8132F/8164F/7024/7048/7024P/7048P/7024F/7048R/7048R-RA/M6348/M6220/M8024/8024/8024F/M8024-k switches. Dell PowerConnect series switches closely conform to networking industry standard operational capabilities and administrative interfaces. The differences below should be studied carefully as attempting to configure or operate the PowerConnect switches in the same manner as for previous releases of firmware for PowerConnect 8132/8164/8132F/8164F/7024/7048/7024P/7048P/7024F/7048R/7048R-RA/M6348/M6220/M8024/8024/8024F/M8024-k switches may lead to unexpected results.

Release 5.1.0.1

- IGMP Snooping

  IGMP snooping is enabled by default.
  Traffic addressed to reserved multicast IP addresses is flooded.
  Unregistered multicast is flooded to all ports in the VLAN until a multicast router port is identified.
  Once mrouter port is identified the traffic is forwarded to mrouter port and listener ports only.

- PIMSM

  PIMSM Rendezvous Points can be positioned anywhere in the network, not just as the first hop router. Although multiple Rendezvous Points can be configured, only one Rendezvous Point is active at any time.

- Auto-Configuration

  Auto-configuration recognizes any of the assigned internal switch's MAC addresses when present in an auto-configuration file. The switch re-writes the file to use the base MAC address of the switch.

- Dot1x Clients

  The maximum number of 802.1x clients (i.e. supplicants) that can be authenticated per port is increased to 24. This increase does not include a corresponding increase in the maximum number of 802.1x clients that are supported on an entire switch or stack.

Release 5.0.1.3

- No Changed Functionality in this Release

Release 5.0.0.4

- Stacking Ports Change

  The maximum number of ports that can be configured for stacking per switch is limited to 8. This is done to ensure that the Hardware limits for maximum stack trunk members are not exceeded.

- Stacking Over QSFP+ Ports

  Stacking is supported over standard QSFP+ ports at either 1x10G or 4x10G mode. The ports must be configured as stacking ports.

- Bootcode upgrade

  Bootcode program is enhanced to automatically upgrade bootcode on migrating switches from pre-4.x version to 5.x version.

Release 4.2.2.3

- No Changed Functionality in this Release

Release 4.2.1.3

- VoIP Phone Limits

  The limitation on the number of VoIP phones has been increased to 576 phones for the PowerConnect 7024/7048/7024P/7048P/7024F switches.

Release 4.2.0.4

- LAG Limits

  Ports can be formed into LAGs in a more flexible manner. The system supports up to 128 total LAGs. Up to 144 ports can be assigned to dynamic LAGs. Up to 72 LAGs can be configured as dynamic. A LAG may contain up to 8 ports. The M8024 supports 12 total LAGs (static or dynamic) with up to 24 ports assigned to dynamic LAGs.

- Stacking Over Ethernet Ports only on M8024-k/8024/8024F

  Stacking is supported over standard Ethernet SFP+ ports. The ports must be configured as stacking ports.

- iSCSI Default Changes

  iSCSI optimization is enabled by default. iSCSI optimization will reconfigure ports that are attached to Dell EqualLogic arrays to utilize spanning-tree portfast and unicast storm disable.

Release 4.1.1.9

- No Changed Functionality in this Release

Release 4.1.0.19

- PHY microcode upgrade process

  The PHY microcode upgrade process has been enhanced to upgrade the PHY microcode to the latest version based on PHY revision. If the user experiences problems links on the combo ports after the upgrade completes, a reboot may be required in order to activate the new PHY firmware.

- Asymmetric flow control

  Asymmetric flow control is implemented for the PC8024X, PCM8024, PCM6348, PC70XX, and PCM8024-k switches. The switch does not generate pause frames when congested. It will honor pause frames as per industry standards.

Release 4.1.0.6

- Authentication

  The enable and line authentication methods will no longer perform authentication if a password for the method is not configured. Previously, these methods would always succeed if no password was configured. To achieve the same functionality, add the "none" method to the list after enable or line method.

  The default authentication list for telnet and SSH has been changed to enableNetList. The only authentication method contained in enableNetList is enabled. The net effect of these two changes is that a password is required to enter privileged exec mode when using telnet or SSH.

  Administrators wishing to maintain the previous PowerConnect behavior can set the default authentication list for telnet and SSH to enableList, which has the enable and none authentication methods (no password required to enter privileged exec mode). The following commands change the telnet authentication method to enableList.

```
console(config)# line telnet
console(config)# enable authentication enableList
console(config)# exit
```

- New Web Interface

  The Web interface has been enhanced with new navigation features for ease of use.

- CLI Syntax Changes

  The CLI has changed significantly to be compatible with the PowerConnect switch standard CLI. Configurations for previous releases may not be compatible with this release and may need to be updated. Refer Configuration Migration document for more info.

- Unit/Slot/Port Naming Conventions

  In-band interfaces are named based on stack unit, slot, and port. Units range from 1-12. Slots range from 0-2. Ports range from 1-48. Slots for plug-in modules are numbered 1 and 2. Fixed ports belong to slot 0.

  The service port is still addressed using the *out-of-band* keyword.

- Management VLAN Deprecated

  The PowerConnect series switches do not have an in-band management VLAN by default. Administrators can designate a VLAN for support of in-band management operations.

- VLAN interface configuration mode enables routing

  When executing the "interface vlan x" command, routing is automatically enabled on that VLAN.

- Service/Out-of-band Ethernet Port Defaults to DHCP Addressing

  By default, the service/out-of-band Ethernet port will attempt to obtain an address via DHCP.

NOTE: It is recommended that administrators attach the service/out-of-band Ethernet port to a physically separate network for out-of-band network management. The service port does not offer routing or switching capabilities nor does it offer enhanced protection from DOS attacks. Configure a VLAN on one or more in-band interfaces for management of PowerConnect switches over the operational network.

- LACP Ports Inactive Until Attached

  Ports in a LAG configured to use LACP (dynamic LAG) remain inactive (discard received traffic) until they become attached to the LAG. LACP ports that are attached to a LAG will enter the discarding state if they become detached from the LAG for any reason.

  Port level configuration for a port that is configured in a dynamic LAG is disregarded. Remove the port from the LAG to restore use of the port level configuration.

  Ports in a static LAG begin forwarding on link up. Ports in a static LAG disregard port level configuration. Configure static LAG functions on the static LAG interface.

NOTE: It is recommended that administrators disable portfast and auto-portfast on physical interfaces configured in a LAG. Portfast and auto-portfast can interfere with an interface entering into LAG mode on a reboot and possibly enable a packet storm.

- Spanning Tree Changes

  Administrators may assign more than 1024 VLANs to MSTP instances. Only VLANs that are configured on the switch will forward traffic.

  The PowerConnect switches implements the 802.1Q-2005 standard which builds on 802.1D-2004. 802.1D-2004 incorporates the 802.1t, 802.1w and 802.1s revisions. Port path costs are calculated based on the interface speed as shown below and are dynamically recalculated on interface activation and link speed changes.

  External Port Path Cost values (Port Path Cost in 17.14 of 802.1D-2004) are applicable in STP, RSTP, and MST modes (Ref. Table 17-3 802.1D-2004). Use the *spanning-tree cost* command in interface mode to set the external port path cost.

Link Speed	Default Value
10 Gb/s	2000
1 Gb/s	20000
100 Mb/s	200000
10 Mb/s	2000000
1 Mb/s	20000000

  Internal Port Path Cost values are specific to MST mode only (Ref. Table 13-3 802.1Q-2005). Use the *spanning-tree mst <instance> cost* command in interface mode to set the internal port path cost.

Link Speed	Default Value
10 Gb/s	2000
1 Gb/s	20000
100 Mb/s	200000
10 Mb/s	2000000
1 Mb/s	20000000

- User Configurable CLI Banners

  Administrators may configure banners for the following: MOTD, login, and exec. The banners may consist of multiple lines of text. Each new line will consume an extra two characters (CR/LF) that count against the maximum length banner that can be configured.

- Captive Portal

  Captive portal has been extended to support user logout and localization.

- 802.1Q

  The following changes have been made to the operation of VLANs.

  VLAN Membership:

  By default, trunk ports participate in all VLANs. VLANs created after a trunk port is created are added to all trunk ports. VLANs deleted are removed from all trunk ports. The operator may configure a trunk port to explicitly disallow certain VLANs.

  Native VLAN Configuration on Trunk Ports:

  It is now possible to configure the native VLAN on a port in trunk mode. Trunk mode ports will accept untagged frames but will always transmit tagged frames. It is also possible to configure a trunk port to drop untagged frames by filtering on the native VLAN, e.g. by using the *switchport trunk allowed vlan remove* command.

Switchport Mode Configuration Preserved:

When switching between switchport modes (access, trunk, and general), the switchport configuration applicable to the selected mode is maintained. This means that when switching from one mode to another and back, the port will have the same configuration as it had in the original mode. Only the configuration applicable to the selected mode is active on the port.

- VRRP

The following enhancements have been made to the operation of VRRP to increase usability and robustness of operation in the network:

Preemption Delay:

Per the VRRP RFC 3768, when preemption is enabled, the backup router discards advertisements until the master down-timer fires. When the preemption delay timer is set to a non-zero value and the backup switch receives a PDU with a lower priority from the master, then backup switch waits for the preemption delay value before advertising itself as the master.

Timer Advertisement Learning:

In VRRP, all participating routers should be configured with coherent advertisement timer interval values. The operator can now enable timer learning which causes a backup router to learn the master advertisement interval and change its master down interval accordingly.

Ping-able VRRP Interfaces:

RFC 3768 specifies that a router may only accept IP packets sent to the virtual router's IP address if the router is the address owner (master). In practice, this restriction makes it more difficult to troubleshoot network connectivity problems.

This capability adds support for responding to pings by the VRRP master, but does not allow the VRRP Master to accept other types of packets. A configuration option controls whether the router responds to Echo Requests sent to a VRRP IP address. When enabled, the VRRP master responds to both fragmented and un-fragmented ICMP Echo Request packets. The VRRP master responds to Echo Requests sent to the virtual router's primary address or any of its secondary addresses. When the VRRP master responds with an Echo Reply, the source IPv4 address is the VRRP address and source MAC address is the virtual router's MAC address. The VRRP master does not respond to pings sent from the master.

Members of the virtual router who are in backup state discard ping packets destined to VRRP addresses, just as they discard any Ethernet frame sent to a VRRP MAC address.

Fragmentation and Reassembly:

Fragmentation and reassembly of VRRP packets is not supported.

- DHCP Relay

The following enhancements have been made to the operation of DHCP Relay to bring the implementation into conformance with RFC 4649:

DHCPv6 Relay Circuit Id/Remote Id Types

RFC 4649 specifies the IANA assignment of the Relay Circuit Id sub-option and Remote Id option. The implementation has been changed so that the administrator can no longer assign a numerical value to these TLVs as the IANA assigned number is now used. The administrator can still enable or disable the insertion of these TLVs in messages sent to the DHCP server.

Relay Information Option:

The operator has the ability to enable DHCP Relay Information Options both globally and on a physical interface. The interface configuration overrides the global configuration for the selected interface.

Relay Information Option Check:

When DHCP Option-82 insertion is enabled for a relay agent, the server should echo received Option 82 unaltered back toward the client. The relay agent is required to strip Option 82 information before relaying the BOOTPREPLY to the DHCP client. When enabled, the Relay Information Option Check will cause the BOOTPREPLY packet to be dropped if invalid sub-options are echoed by the DHCP server.

- L2 Address Table

The administrator can disable MAC address table aging.

The administrator can configure static forwarding of a MAC address on a specific VLAN.

NOTE: By default, multicast frames are flooded by the switch. Utilize the *mac address-table multicast filtering* command to disable flooding of multicast frames.

- LLDP Enhancements

Multiple Neighbor Support:

Multiple neighbors are supported on a single LLDP interface. The number of recognized neighbors is limited to two per port or 834 LLDP neighbors on a fully stacked set of switches. There is no restriction on the number of neighbors connected to an LLDP port. If more LLDP neighbors are present than are supported, then only the last two neighbors that communicate with the local LLDP interface are recognized and any additional neighbors are ignored.

EEE Support:

Support is added to process/communicate the EEE TLV to partner devices. The EEE TLV is an 802.3 organizationally specific TLV used to report on the EEE Data Link Layer capabilities.

LLDP-MED Support:

LLDP-MED uses LLDP's organizationally specific TLV extensions and defines new TLVs which make it easier to deploy VoIP in a wired or wireless LAN/MAN environment. The LLDP implementation supports the following TLVs:

Mandatory 802.1AB TLVs

- Chassis ID TLV (subtype shall default to MAC Address)
- Port ID TLV (subtype shall default to MAC address
- TTL TLV
- MAC/PHY configuration/status TLV
- End of LLDP PDU

Optional 802.1AB TLV

- Systems Capabilities TLV
- Power via MDI TLV
  NOT recommended for transmission in order to conserve LLDPDU space.

Mandatory LLDP-MED TLVs

- LLDP-MED Capabilities TLV
  This TLV allows the network connectivity device to definitively determine whether particular connected devices do support LLDP-MED and to discover which specific LLDP-MED TLVs the particular end point devices are capable of supporting as well as what specific device class they belong to.
- Network Policy TLV
  This TLV allows the device to advertise its VLAN and associated Layer 2 priority and Layer 3 DSCP attributes which apply for a set of specific protocol applications on this port.
- Location Identification TLV
  This TLV provides the advertisement of location identifier information Class II endpoint Devices. This is expected to be related to wire map or similar network topology data, such that the configuration of the network Connectivity device is able to uniquely identify the physical location of the connected MED endpoint.
- Extended Power-via-MDI TLV
  This TLV allows for advanced power management between endpoints and network connectivity devices. It transmits fine grained power requirement details. This TLV provides significantly more value than the 802.1AB Power via MDI TLV.
- EEE TLV
  The EEE TLV is used to exchange information about the EEE Data Link Layer capabilities. Devices that require longer wake up times prior to being able to accept data on their receive paths may use the Data Link Layer capabilities to negotiate for extended system wake up times from the transmitting link partner. This mechanism may allow for more or less aggressive energy saving modes.

- Dynamic VLAN Assignment

  Dynamic VLAN assignment is intended to support the connection of hosts to a router with enhanced levels of service, typically either security or QoS. This release supports dynamic VLAN assignment as assigned from the RADIUS server as part of port authentication. The following additional checks are performed in support of dynamic VLAN assignment:

  Before assigning the port to RADIUS assigned VLAN, dot1x checks if the given VLAN is in the VLAN database or not. If the assigned VLAN is not in the VLAN database and dynamic VLAN assignment is enabled, a VLAN is created on the port over which the client is authenticated. Each time a client is de-authenticated on an interface with a particular VLAN, a check verifies if there any other interface which a VLAN member is. If there is no interface as a member, the VLAN is deleted. This behavior is same for MAC based authentication as well.

- Usability Enhancements

  In the output of the *show running-config* command, the slot and member configuration is commented with the switch/slot type in human comprehensible form.

  When in interface config mode, CLI users can navigate to a different interface by entering the appropriate interface command without leaving interface config mode.

  CLI users can log out of the switch using the *exit* command (*exit* is an alias for *quit*).

  The CLI Reference Guide is updated with acceptable character sets and maximum lengths for string parameters to commands.

  Management ACLs permit specification of *service any* as shorthand for enabling all services access for in-band management.

  VLANs may be administratively assigned to MSTIs in excess of the switch physical limits and without regard to whether the VLAN is actually configured. Frames are only forwarded on VLANs assigned to interfaces.

  Administrators can re-enter SYSLOG server config mode for a particular SYSLOG server entry without requiring the deletion and re-creation of the entry.

  Administrators can configure the web timeout by navigating to: System -> Management Security -> Telnet Server -> Telnet Session Timeout.

  User configured banners (login, exec, MOTD) appear in the running config.

  By default, auto-install supports image downgrade for network installs, specific version USB installs (using a .setup file), and stack firmware synchronization.

  A comprehensible message and recommendation is issued when configuring multiple services (telnet, http, etc.) to listen on the same TCP port.

  The *terminal length* command allows user control over terminal paging.

- Simple Mode

The PowerConnect M8024-k is the only modular switch that defaults to the simple mode of operation. Simple mode contains a restricted set of commands suitable for control of a port aggregation device that can be deployed in a network without requiring updates to the network by a network administrator. Users needing switch capabilities which require the network administrator to modify the network configuration can exit simple mode using the *no mode simple* command.

- AAA Authentication

  In prior releases, more than one method could be specified for dot1x authentication even though only the first method was attempted. The CLI and Web now only accept a single method for dot1x authentication.

Issues Resolved

The following issues from previous releases have been corrected. The issues listed here may have been discovered on any of the switches listed on the title page.

Release 5.1.0.1

Summary	User Impact	Resolution	Affected Platforms
M6220 crashes when issuing command “show interfaces switchport po1”	Switch crashes when using this command	Fixed memory issue in a loop	All 5.0 supported platforms
Cannot apply ACL on VLAN 'out bound' direction from GUI	User needed to use CLI	Fixed the issue to be able to apply in both directions from the web	All 5.0 supported platforms
Default VLAN cannot be made static from GUI	Cannot change VLAN member ports settings	Fixed VLAN membership web page	All 5.0 supported platforms
Incorrect SFP interface log messages on stack	The wrong port may get reported in the trap notification	Calculate the correct internal interface number	Platforms that support XFP, SFP and SFP+ transceiver modules
SNMP management IP address can only be set from WebUI and lost after reboot.	command is missing in the CLI in Simple Mode	Added CLI command support	All 5.0 supported platforms
Simple mode In-band IP address missing after reboot.	"ip address vlan" command disappears from the running-config after reboot	Put "ip address vlan" after "port-aggregator group" commands in the text config	PCM6220 PCM6348 PCM8024 PCM8024-k
ARP entries are purged for unknown reason	L3 egress objects are not programmed correctly resulting in incorrect L3 forwarding.	Use the SDK init function to set defaults for egress object.	All 5.0 supported platforms
OOB Static IP unreachable after stack failover	After failover stack loses static IP address configured on OOB interface.	Proper checks prevent using the previous DHCP mode.	All platforms that support the OOB interface

http[s] authentication against RADIUS only allows privilege level 1 access	HTTPS authentication through RADIUS grants only read-only access.	parse RADIUS server response properly	All 5.0 supported platforms
SNMP v1/2 community manager address no longer functions with network address.	When a subnet IP is set as SNMP community IP address then snmp requests from hosts of that subnet are not accepted on the box.	Get the mask from the community IP address configured and set it instead of the hard coded value.	All 5.0 supported platforms
Switch service tag not displayed by “show system id” command	Switch service tag not displayed with “show system id” command	Added retry to get the Service Tag value	M8024-k, M8024, M6348
CLI commands are not authorized after Password Recovery	Enabling password recovery will not allow the user to run CLI commands on the serial console.	Fixed the issue to enable commands from serial console also	All 5.0 supported platforms
LINK UP on all interfaces during POST,	Links are UP and flapping during power reset and reloads.	Changed the CPLD and reset logic	PC8024 and PC81xx
FCoE -M8024-k setting TSA map to link strict and assigning bandwidth allocation to TC	In the CEE mode there is no way to specify the TSA mode in the ETS TLV	Check if any weight is configured for the TCGs, if so set the mode to ETS.	Platforms running DCBX and including ETS
Switch GUI forcing 100Mb speed on External ports when cloning port configurations	Switch GUI set all external ports to 100Mb speed when cloning port configurations.	Corrected port speed processing from WEB	M6348
PowerConnect M6348/General port GUI issue	Vlan membership information on web is displayed and applied incorrectly	Javascript fixed to pick correct enum values	M6348
M6348 - service tag not displayed in GUI	Service tag shows up as none on GUI	Synchronization issue fixed to retry and get the tag information	M6348
email addresses with underscore "_" are rejected	A valid email id with an underscore cannot be used	Underscore is now considered valid character	All 5.0 supported platforms
phone port configuration macro incomplete	The macro never returns and appears to hang	Fixed the issue and return error	All 5.0 supported platforms

Release 5.0.1.3

Summary	User Impact	Resolution	Affected Platforms
Re-enable Auto Negotiation using GUI doesn't work properly	The Auto Negotiation can't be enabled back on "Port Configuration->Show All" page once it has been disabled.	Corrected error in Port Configuration page.	All 5.0 supported platforms

VLAN ACL blocks traffic across stack members	ACL prevented traffic from reaching destination	Prevented VLAN ACL from being applied to stack ports.	All 5.0 supported platforms
Power supply logging	Power Supply messages are only sent to the log file.	Elevated failure messages to ERROR severity	All 5.0 supported platforms
'no ipv4 or ipv6 address found in response for request id' error	'no ipv4 or ipv6 address found in response for request id' error message flooding the switch	Corrected problem that was causing extra error messages to be displayed.	All 5.0 supported platforms
phone port configuration macro incomplete	The phone port is missing some needed commands	Added missing commands to the pone port macro.	All 5.0 supported platforms
web session timeout	Web session would timeout regardless of the timeout setting	Corrected the hard timeout to be one hour.	All 5.0 supported platforms
RX Equalizer setting on Stacking ports.	RX Equalizer was not set on the stacking port which caused stacking errors to be reported.	Added RX Equalizer value.	All PC70XX Switches
interface speed options	Invalid speed options message is not clear	Changed the message reported when an invalid speed option is input.	All 5.0 supported platforms
Change PoE Disconnect Type to DC disconnect	PoE controller Disconnect Type was changed to DC Disconnect.	PoE controller Disconnect Type was changed to DC Disconnect.	PC7024P PC7048P
stacking with extension modules	Stacking with redundant stack rings caused packet flooding on the stacking links.	Corrected problem with stack link queuing.	All 5.0 supported platforms
DHCP Req pkts are not being forwarded to Voice VLAN Component	When using Avaya phone on a switch running dot1x, the phone will NOT get authenticated and thus will not boot	Corrected DHCP forwarding problem.	All 5.0 supported platforms
Netlogic memory and B0 CPU support	Netlogic memory and B0 CPU support	Added support for Netlogic memory and B0 CPU.	PC8132 PC8132F PC8164 PC8164F

Release 5.0.0.4

Summary	User Impact	Resolution	Affected Platforms
OpenManage UI does not accept blank space character for port description	Port description does not accept space	Correction the port description validation to accept spaces.	All 4.2 supported platforms

"show spanning-tree detail" counters are non-zero for inactive interfaces	The user may think that there is traffic over interfaces that are supposed to be inactive as far as spanning tree is concerned.	Corrected the counters.	All 4.2 supported platforms
Unable to remove 0.0.0.0 as default gateway on OOB interface using the web.	The user may not be able to remove the default gateway for the OOB interface causing unwanted traffic to go over the OOB interface.	Added support for setting the gateway to 0.0.0.0.	All 4.2 platforms that support the OOB interface
When connecting via SSH, the user is not prompted to acknowledge the MOTD	The user may log in without having acknowledged the MOTD.	Add functionality to send the acknowledge question when new SSH connection is created, but after authentication.	All 4.2 supported platforms
"encapsulation" command is unavailable in interface range mode	The user could only set VLAN encapsulation on a single VLAN at a time.	Added support for the encapsulation command in interface range VLAN mode.	All 4.2 supported platforms
M8024-k OpenManage Web UI stack view display	The user could not get accurate information about a stack of M8024-k switches from the stack view web page.	Corrected the information displayed on the stack view web page.	PCM8024-k
"spanning-tree transmit hold-count" command's value is not reflected in show command	The user could not see the configuration of the hold-count parameter.	Corrected the output of the "show spanning-tree detail" command to include the configuration of the hold-count parameter.	All 4.2 supported platforms
Inconsistent behavior in single and range interface mode of "spanning-tree port	The user may be able to configure an invalid spanning tree port priority in range mode.	Corrected the error handling so that the invalid priority is not used.	All 4.2 supported platforms
CLI command "no passwords strength exclude-keyword" requires <keyword>	The user could not reset the excluded keywords to the factory default of no excluded keywords with a single command. It was necessary to remove each excluded keyword one at a time.	Correctly implemented the "no" form of the "passwords strength exclude-keyword" command.	All 4.2 supported platforms
Inline help for "spanning-tree loopguard" is incorrect.	The help text might lead the user to think the command only applied to a single port instead of all ports.	Corrected the help text so that it indicates that the command applies to all ports.	All 4.2 supported platforms
Some of the options of "show ip pim" command are not available in user EXEC mode.	Some of the options of "show ip pim" command are not available in user EXEC mode.	Added missing options to the CLI tree.	All 4.2 supported platforms

Configuration command "logging <hostname>" accepts more than 63 characters.	Configuration command "logging <hostname>" accepts more than 63 characters, but saves only 63 characters in running-config.	Added checks to return error when hostname is larger than 63 characters.	All 4.2 supported platforms
dot1dTpPortMaxInfo is displaying maximum frame size that includes MAC header.	dot1dTpPortMaxInfo is displaying maximum frame size that includes MAC header.	Excluded the MAC header length when retrieving the OID information	All 4.2 supported platforms
If a user attempts to create a certificate request with information that is not identical to the key generated, the user is not given an error/ informative response letting them know there is a conflict between their key and their request.	No error message was given.	Added a message once an exit is issued from the request or generate command. This is to tell the user whether the operation was successful or not.	All 4.2 supported platforms
OIDagentInventorySupportedUnitExpectedCodeVer provides incorrect display string 1.0.176.0	agentInventorySupportedUnitExpectedCodeVer object returns incorrect values.	Made the OID that is in private MIB obsolete as it's not required.	All 4.2 supported platforms

1. Changes are not applied to the correct interfaces on the pages "System->sFlow->Sampler Configuration" "System->sFlow->Poll Configuration" 2. Incorrect error message is displayed when not configured Receiver index is applied to interface on "System->sFlow->Poll Configuration" page.	1. Changes were not applied to the correct interfaces on the GUI pages referred to. 2. An incorrect error message was displayed.	1. Used initialized buffers. 2. Correct the error message.	All 4.2 supported platforms
"show ip route configured ...longer-prefixes" reports that default gateway is not configured, which is incorrect.	The default gateway would not be shown on executing "show ip route configured"	Corrected the implementation of this command so that it functions correctly.	All 4.2 supported platforms
CLI command "show ip route 192.168.2.2 /24" not ignoring host bits.	The user would not always get the correct list of routes from the "show ip route" command.	Corrected the logic in the implementation of the "show ip routes" command so that the appropriate list of routes are shown, depending upon which optional parameters are given.	All 4.2 supported platforms
CLI command "show spanning-tree detail" missing information.	The user could not see the configured values for spanning tree max hops.	Changed the output of the "show spanning-tree" and "show spanning-tree detail" commands to include the configured value of max hops.	All 4.2 supported platforms
"ipv6 pim join-prune interval" command does not work	The user could not change the configuration of the IPv6 PIM join interval.	Corrected the implementation of this command so that it functions correctly.	All 4.2 supported platforms
Macro input string does not accept more than 20 characters	The interface string length is limited to 20 characters for the "macro global apply" command.	Increased the acceptable string length for the "macro global apply" command to 256 characters.	All 4.2 supported platforms
startup-config failed error message is displayed when finishing the Dell Easy Setup Wizard	startup-config failed error message is displayed when finishing the Dell Easy Setup Wizard	Corrected the implementation of this command so that it functions correctly.	All 4.2 supported platforms

In stacking environment, "show system temperature" command output is corrupted	CLI output for command "show system temperature" is corrupted when pagination is used.	Corrected pagination in the command handler.	All 4.2 supported platforms
Error message for port enable / disable on IE on 8024F combo ports	When a copper port was disabled, port was getting set in no negotiating mode.	Corrected by disabling negotiation on combo ports	PC8024F
Alignment issues in the output of "show voice vlan interface" command	The alignment issues make it difficult for the customer to read the page.	Corrected alignment issue	All 4.2 supported platforms
CLI command "show ip igmp snooping" output is truncated.	The displayed info is not complete on page.	Corrected the implementation of this command so that it functions correctly.	All 4.2 supported platforms
vrrp ip command accepts invalid IP addresses	Switch allowed user to misconfigure VRRP IP	Added checks to return error when invalid VRRP IP address is given.	All 4.2 supported platforms
CLI command "isdp enable" does not work for a range of ports	User cannot enable isdp on range of interfaces	Added support to "isdp enable" command in interface range mode	All 4.2 supported platforms
"show interface Priority-Flow-Control" command output is not formatted correctly	The user sees the info but it looks messy and is hard to read.	Corrected formatting issues	PC8024 PC8024F PCM8024-K
CLI command "show ip route 192.168.2.2 /24" not ignoring host bits.	The user would not always get the correct list of routes from the "show ip route" command.	Corrected the logic in the implementation of the "show ip routes" command so that the appropriate list of routes are shown, depending upon which optional parameters are given.	All 4.2 supported platforms
Port channel goes down during master failover.	The members of the stack other than the master unit and their port channels, i.e. the Standby units and their port channel interfaces, are now not affected by a master failover and the port channel stays up during failover.	Corrected the logic to check for active port channels in the new Standby master unit.	All 4.2 supported platforms
switches rebooting - possible crash dump w/ emWeb	The switch crashes when it receives the url with the maximum characters.	Corrected URL length problem	All

general mode vlan does not show up after a reload, it shows up in access vlan	The general mode for switchport won't work properly in several cases, such as, script apply, nsf failover and save and reload.	Corrected memory initialization problem	All
SNMP OIDs 1.3.6.1.4.1.674.10895.3000.1.2.110.7.x causing switch crash	Walk of any member of envMonFanStatusEntry and envMonSupplyStatusEntry with 67109251 index causes crash.	Corrected unit number range check.	All
Stack ARP Problem	ARP replies to a routing interface are not received at the CPU after clearing the config and reconfiguring the routing interfaces.	Corrected ARP reply policy problem	All
Stack member units port display is missing in web GUI.	Stack member unit ports were not displayed properly.	Corrected power LED element id name problem which was causing this display problem.	PCM8024-K
No response to ICMP with jumbo (ping)	Third IP fragment was being dropped in jumbo Ping packet.	Corrected jumbo Ping packet problem.	All
Ports connected to Intel X520 NIC do not return online after reboot.	When customer is using the Intel X520 NICs, sometimes the ports never came back up after a reboot of the switch.	Corrected port configuration timing issue.	PC8024 PC8024F
switch reboots randomly	switch reboots randomly	Corrected memory corruption problem.	All

Release 4.2.2.3

Summary	User Impact	Resolution	Affected Platforms
IP routing unexpectedly after reboot despite its not having been enabled.	Traffic will get forwarded by software when global routing is not enabled.	Correct the default action so that global forwarding is enabled for the hardware.	All 4.2 supported platforms
Telnet existing session is interrupted when "New Telnet Sessions" is set to "Block".	"New Telnet Sessions" are changed to Block, All the current telnet sessions are closed and using "Telnet Server Admin Mode" to set Disable will only block new telnet sessions.	Functionality was corrected so that "New Telnet Sessions" will only block new telnet sessions and "Telnet Server Admin Mode" will close all the sessions if the mode is Disabled.	All 4.2 supported platforms
OOB interface unreachable after failover	Out-Of-Band interface will be unreachable after a stack failover	Corrected MAC address for new manager.	PCM6220 PCM6348 PCM8024 PCM8024-k
Switch CLI help does not locate the 'initiate failover' command properly	Warning message printed during execution of the deprecated "movemanagement" command incorrectly states that "initiate failover" command is executed from privileged EXEC mode whereas it's available from stack config mode only.	Corrected the warning message	All 4.2 supported platforms

Timeout during SNMP walk on root	SNMP walk on root ends with timeout	Corrected delay that caused timeout.	All 4.2 supported platforms
"show interfaces switchport" command shows incorrect General Mode Tagged VLANs value	"show interfaces switchport" command shows incorrect General Mode Tagged VLANs value.	Corrected the display of the General Mode Tagged VLANs value.	All 4.2 supported platforms
Error while adding an access-list to an access-group	Error message when trying to apply ACLs to VLANs.	Corrected the condition that resulted in the error.	PC8024 PCM8024 PCM8024-k
Walk of agentDaiVlanStatsTable returns statistics for all the 4096 VLANs	Walk of agentDaiVlanStatsTable returns statistics for all the 4096 VLANs even they do not exist in the system	Corrected the VLAN Stats Table data.	All 4.2 supported platforms
OOB interface configured with default IP via Setup Wizard though not to do so	When the Setup Wizard is used the OOB interface IP address is incorrectly set to 192.168.2.1 static IP by default	Corrected the setting of the OOB interface IP address.	All 4.2 supported platforms
Unable to create VLAN ID and name VLAN in Web GUI	Unable to create new VLAN with its name using the Web GUI	Corrected the VLAN creation GUI	All 4.2 supported platforms
"Failed to get CPU cosq 0 drop counters, error -16" messages in logs	"Failed to get CPU cosq 0 drop counters, error -16" messages in logs	Corrected the retrieval of cosq 0 counters.	All 4.2 supported platforms
Default "ip address dhcp" command on VLAN 1 causing "failed to bind socket" error repeatedly	Default "ip address dhcp" command on VLAN 1 causing "failed to bind socket" error repeatedly	Corrected DHCP socket problem.	All 4.2 supported platforms
agentPortSpeedDuplexStatus SNMP MIB object documentation error	Mistakes in the agentPortSpeedDuplexStatus SNMP MIB object description	Corrected MIB object description.	All 4.2 supported platforms
ifIndiscards is still counting VLAN discards if the interface switchport mode is in trunk mode	ifIndiscards is still counting VLAN discards if the interface switchport mode is in trunk mode (acceptable frame type is all)	Corrected ifIndiscards counter collection.	All 4.2 supported platforms

Switch doesn't register all the 576 devices if LLDP-MED has all the optional TLVs.	Switch doesn't register all the 576 devices if LLDP-MED has all the optional LLDP-MED Location TLVs.	Corrected the allocation of LLDP-MED Location TLVs.	All 4.2 supported platforms
SNMP and LOG errors when setting ifAdminStatus	When setting ifAdminStatus “adminState 2d is not valid” errors are produced.	Corrected error check when using invalid testing options.	All 4.2 supported platforms
Cannot type input into external serial connector after reboot of switch	After reboot external serial connection can become inoperative.	Corrected initialization of serial connection.	PCM6220
Web GUI doesn't display port 24 if using Internet Explorer 9	Device View doesn't display one port on IE 9. (IE9 is currently unsupported)	Corrected problem for IE9.	All 4.2 supported platforms
Switchport general configuration, VLAN1 tagged not saved in running config	"switchport general allowed vlan add 1 tagged" is not displayed in running config	Corrected check of enabled VLAN.	All 4.2 supported platforms
Cannot rename vlan1	Cannot rename vlan1 running v4.2.1.3. It is correct that the default VLAN cannot be renamed (same as a Cisco switch).	Updated error message to reflect this behavior.	All 4.2 supported platforms
SNMP Port tag/untag issue	When setting VLAN un-tagging for a specific port using the dot1qVlanStaticUntaggedPorts object, All the other ports are automatically added to that particular VLAN as tagged.	Corrected the port un-tagging set.	All 4.2 supported platforms
DNS client error in logs and switch locks up and needs to be rebooted.	Upgrade of 3.1.4.5 to 4.1.0.6 DNS client error “osapiSocketRecvFrom returned error “ in logs and switch locks up and needs to be rebooted.	Corrected service port link status during upgrade.	All 4.2 supported platforms
Terminal Length setting not working as in 4.1	Terminal length is not setting per-session is an enhancement scheduled for the next release.	Corrected a problem with terminal scrolling.	All 4.2 supported platforms
Trunk port multiple vlan assignment doesn't work properly after reboot	Trunk port multiple VLAN assignment doesn't work properly after reboot.	Corrected command parsing problem.	All 4.2 supported platforms
FIP snooping session is not getting established after script apply.	FIP snooping session is not getting established after script apply.	Corrected FIP snooping command problem.	All 4.2 supported platforms

"ip http secure-server" command not getting migrated from 4.1.0.19 build to 4.2.1.3 build.	ip http secure-server command not getting applied when we migrate from 4.1.0.19 to 4.2.1.3 release	Corrected command parsing problem.	All 4.2 supported platforms
Data loop in Simple mode when adding VLAN	A data loop occurs in the port-aggregator if a new VLAN is added to an interface.	Corrected the VLAN creation error.	PCM6220 PCM6348 PCM8024 PCM8024-k

Release 4.2.1.3

Summary	User Impact	Resolution	Affected Platforms
The “show fiber optical-transceiver" command shows LOS even though link is up.	The “show fiber optical-transceiver" command was reporting incorrect values when optical transceivers that did not support diagnostics were used.	Correct diagnostics so that diagnostics for unsupported transceivers are not displayed.	All 4.2 supported platforms
Unable to ping with jumbo frames set	MTU size configured on the combo ports will be lost after a save and reload and also when changes the media preferences are made.	Corrected the storing of the MTU size	PC72xx and PC80xx platforms
cpCaptivePortal WebLangCode. 1.1 displays en when mib says only supported value active (1)	The description of the cpCaptivePortalConfigWebLangCode object doesn't correspond to the values it returns.	Corrected the description in the fastpath_captive_portal.mx file	All 4.2 supported platforms
LLDP Assignment of port ID for Port-Description TLV	When Port-Description is set as no description in LLDP port configuration, the TLV should contain the Port Interface name as the port description by default instead of 0.	Corrected the default Port-Description.	All 4.2 supported platforms
The CLI shows incorrect media type 10GBASE-T for fiber ports	The "show interface advanced firmware" shows incorrect information under "Type" column.	Removed the Type column which was not valid.	All 4.2 supported platforms
Can't assign a name to a VLAN	Config migration for the "name <vlan name>" command was not correct.	Corrected the config migration for the "name <vlan name>" command.	All 4.2 supported platforms
No default route or static showing in ip route table	"Show ip route" commands will not display route even though there were routes is in the router(static routes, ospf routes) for terminal length 0.	Corrected the display of the "Show ip route" command.	All 4.2 supported platforms

CLI command "show dot1x users" is missing	CLI command "show dot1x users" is missing	Corrected the command tree for the "show dot1x users" command.	All 4.2 supported platforms
Missing port membership from SNMP (dot1qVlanStaticUntaggedPorts and dot1qVlanStaticEgressPorts)	Changing VLAN configuration for general mode affected trunk mode configuration and there from the port membership returned via SNMP.	Corrected the issue.	All 4.2 supported platforms
The VRPP track port priority changes in the running config	The VRRP track port priority in the running config is retrieving the operational value instead of the configured value.	Corrected the retrieval of the configured value	All 4.2 supported platforms
Firmware won't allow domain names with hyphen "-" in logging email	The hyphen is part of the allowed characters available for the email address.	Added the hyphen to the allowed characters for email addresses.	All 4.2 supported platforms
Internal ports are up during most of the switch POST	Internal ports were up while switch is booting, this was causing traffic loss in network.	Corrected the initialization of the internal ports. CPLD Code Update is required. 1. Update the CPLD using the command 'dev cpldUpdate' Console#dev cpldUpdate 2. Power cycle the switch. (Power Cycle from CMC WebUI. Do not run “reload” from the console prompt)	PCM8024-K
Continuous log message at default settings	POE log message comes up during power up sometimes.	Removed unwanted message.	PC7024P/PC7048P
DNS client error	The meaning of the DNS error message: “DNS Client: osapiSocketRecvFrom returned error for addr 0x1214BCA8” is unclear.	Corrected the text of the message.	All 4.2 supported platforms
VRRP Intermittent Connectivity Issues	Ping to a remote host will not work if switch acts as VRRP master	Corrected a VRRP communication issue.	All 4.2 supported platforms
VLAN membership port names not consistent in GUI	VLAN membership port names are not consistent.	Corrected the port numbers displayed in the GUI.	All 4.2 supported platforms
Radius crash	Sometimes switch crashes when receiving of Radius packets	Corrected the crash.	All 4.2 supported platforms
In a Stack, the "show system temperature" CLI command breaks CLI	CLI output for command "show system temperature" is corrupted when pagination is used because the stack displays much more data.	Corrected the pagination issue.	All 4.2 supported platforms
QOS on port channel	There is no way to see the match packet counts of a policy-map on a port-channel.	Command "show policy-map interface port-channel <port-channel number>" was added.	All 4.2 supported platforms

Dropped VLAN frames are included in Discards counters.	Customer is really not able to use this counter to monitor their network outage activity.	Corrected by not ignoring the dropped VLAN frames in the Discards counter	All 4.2 supported platforms
PC7048 Combo ports are not passing traffic.	Combo ports are randomly not transmitting traffic, but receiving frames when media type preference set as SFP	Corrected by adding a property to bypass the lane initialization when media-type preferences is set.	PC70xx
Order of switchport commands in running-config changed	The "show running-config" command shows the detailed switchport configuration before the switchport mode. This caused problems with some scripts.	Corrected the order of running-configuration output.	All 4.2 supported platforms

Release 4.2.0.4

Summary	User Impact	Resolution	Affected Platforms
PowerConnect sFlow implementation is not per specification	sFlow implementation is not per specification	Issues corrected and passes conformance test	All 4.2 supported platforms
Using config wizard to setup 8024 causes iscsi error messages off out-of-band in console	Doesn't affect any iscsi traffic. Constant log messages with the error "Can't create static rule".	Issue is corrected.	PC8024
8024 stack does not follow similar banner execution for console, telnet and ssh	If a user logs in via console - motd and login banners are executed If a user logs in via ssh - only exec banner is executed If a user logs in via telnet - all 3 banners are executed	Behavior is now as follows: Add motd banner display for telnet connection before motd acknowledge question is asked. Remove motd banner after motd acknowledge question.	All 4.2 supported platforms
Simple Switch should have FC enabled by default	FC not functional	FC is enabled by default in simple switch mode.	All 4.2 supported platforms
OSPF error message after reboot	With 128 IPv4 & IPv6 interfaces & OSFP configured a reboot caused the following error messages to be generated: Failed to send message to OSPF mapping thread in ospfMapRoutingEventChangeCallBack() These lost events could lead to incorrect routing.	Issue has been corrected.	All 4.2 supported platforms

show crypto key mypubkey generates two error messages	After generating DSA & RSA keys, executing the command "show crypto key mypubkey" generates the following error messages: <187> APR 23 09:09:22 192.168.1.2-1 OSAPI[162603392]: osapi_file.c(657) 426 %% File close failed for descriptor 37 <187> APR 23 09:09:22 192.168.1.2-1 OSAPI[162603392]: osapi_file.c(657) 427 %% File close failed for descriptor 37 There is no impact on the keys themselves.	Resolved	All 4.2 supported platforms
Web GUI ARP table does not match the CLI ARP table	The Web GUI does not display the static/local ARP entries. However, once an external port is linked up some, but not all, of the Static/local appear in the Web GUI.	All ARP entries are now shown.	All 4.2 supported platforms
The copper auto negotiation process fails at 100mb FD and fails to link up	The copper ports 1-24 fail on 8024 to negotiate at 100Mb FD.	8024 copper ports negotiate to 100M FD.	PC8024
PCM6220 - Wrong information for current link status in port configuration page on the GUI	The current stacking port status does not display “stacking link up”	The web stack display has been updated to accurately reflect the correct information as well as address some style issues.	All 4.2 supported platforms
PC8024 - VLAN membership change on interface affects unrelated interface	If user changes VLAN membership configuration on trunk port via the WEB he loses ports configuration on access ports and access ports are put into default VLAN.	Issue is resolved.	All 4.2 supported platforms
Implement dot1qVlanStatic Table in M8024-K	The dot1qVlanStaticTable is not available on M8024-k.	the dot1qStaticVlanTable is implemented for the M8024-k	All 4.2 supported platforms
Trunk mode native vlan implementation not compatible with Cisco	Native vlan implementation is incompatible with Cisco. Switch will egress native vlan traffic as tagged and Cisco will drop ingress tagged native vlan traffic.	Implementation of native vlan changed to be compatible with Cisco.	All 4.2 supported platforms
PCM6220 - Switch hangs when user tries to transfer a file from the flash to the server using sftp	Switch hangs and needs a hard reboot.	None – issue is resolved.	All 4.2 supported platforms

No message logged for "Max number of SSH login sessions exceeded"	The switch does not log an error message when the maximum number of SSH sessions has been exceeded. The switch does accept 5 SSH sessions normally, when the 6th session connection is attempted via SSH, the connection is refused, but no error message is logged.	A Log message "Unable to find a free connection. Exceeded the maximum number of allowed connections." has been added.	All 4.2 supported platforms
CLI command "show ipv6 interface" does not paginate correctly	The CLI command "show ipv6 interface" does not paginate correctly when a large number of interfaces/addresses are configured.	Pagination mechanism corrected.	All 4.2 supported platforms
2nd and 4th block of copper ports 5-8 and 13-16 think they are fiber ports, possible problems	Ports report to be fiber ports and not copper ports.	Corrected error checking logic to correctly select fiber ports for fiber diags and copper ports for copper diags.	PC8024/PC8024F
WebGui Secure Shell SSH Remote Access	On the WebGui under Management Security, Secure HTTP, Secure Shell does not work on the Web UI	Issue is corrected	All 4.2 supported platforms
Web UI MSTP Instance pull down menu displays 4k MSTIs	In the "MSTP Interface Settings" page of the Web UI, the Instance pull down menu has a range of 1-4094 MSTIs.	Issue is corrected	All 4.2 supported platforms
Flowcontrol negotiation issues with 10GBase-T module	Flowcontrol negotiation issues between 6200 and 8024/8024F	Driver update applied.	PC8024/PC8024F
PC8024 - GUI - Under Port Configuration page get error on 10GB ports when you change any setting	When you change the port setting, for example the duplex settings or description, from the GUI under switching -> Ports -> Port Configuration you will get outputs error when changing port settings on 10G ports. The popup says 10G speed is invalid. Error message attached. This is a problem with code version 4.1.0.6 under the GUI no problem when using the command prompt.	Erroneous pop-up message removed.	All 4.2 supported platforms
Unable to config secure ssh from web interface. error 'sshcfg_load start' missing pops up	Unable to configure Secure Shell from web interface. Error pops up.	Corrected web page	All 4.2 supported platforms
Web interface fails to provide an iSCSI web page when selecting the iSCSI item.	The web page for iSCSI fails to open when selected with OpenManage. .	Corrected web index page	All 4.2 supported platforms

Line "no passive-interface Vl32" in startup-config does not get loaded on startup	The following is displayed when startup-config is loaded: Applying Global configuration, please wait ... Applying Interface configuration, please wait ... ******* The following lines in "startup-config" failed: ******* Line 57:: no passive-interface Vl32	Corrected stored config	All 4.2 supported platforms
Web GUI Admin Duplex setting on 10G Fiber ports	Switching-->Port-->Port Configuration Select a ten gigabit interface Te1/0/1 and you can see that "Admin duplex" and "speed" are still active and can be changed, but when you apply it gives an error message saying " Error failed to set current auto negotiation with disable".	Invalid selections disabled on page load.	PCM6348
Advertise LLDP Management Address as IP Address assigned to OOB interface	LLDP advertises the switch's MAC address as the Management Address. Request to advertise the management IPv4 or IPv6 address instead.	The following behavior is now implemented: 1) Will advertise service port address if it is there 2) If service port is not there, then will send network address 3) If both of the above are not there and if it is routing interface will send IP address of the routing interface 4) If none of the above not there, will send MAC address.	All 4.2 supported platforms
PCM6348 - Log message output	Messages repeated in the switch logs <190> APR 28 19:39:22 10.1.208.10-1 STATSMGR[239558880]: collector.c(1066) 3445 %% Failure in function collectorGet <190> APR 28 19:39:22 10.1.208.10-1 STATSMGR[239558880]: presenter.c(102) 3446 %% ERROR!! Failure in preStatsGet 0x0002011e <188> APR 28 16:40:31 10.1.208.10-1 ARP[301140128]: ipmap_arp_api.c(855) 3325 %% Received ARP Reply on interface Vl208 with bad target IP address 255.255.255.255. Sender IP is 10.1.209.60, sender MAC is 76:f7:b9:cf:06:7e.	SNMP walk/gets on counters for CPU/vlan routing ports not supported by platform no longer log a warning message	All 4.2 supported platforms
Firmware missing port VLAN membership in the GUI	Port VLAN membership will not be shown in the GUI.	Web code updated to display VLAN membership	PCM6220

M8024 - 1GB link being negotiated on 10GB Intel X520-KX4	The M8024 is negotiating 1GB speed connection with the 10GB X520-KX4 Intel card in the blade server. Issue is only present with new	Incorrect pre-emphasis values have been corrected.	PCM8024
Feature request - Display "client-DUID" in DHCP binding table.	The "Client-DUID" is used to uniquely identify an individual host receiving DHCP address configuration. In the case of a multi-homed host, it is possible to determine that the host has multiple bindings for different interfaces and which interfaces belong to each host.	Client-DUID parameter has been added to show "ip dhcp binding" command output.	All 4.2 supported platforms
clock summer-time recurring EU offset 60 zone "GMT" not offsetting the time by 60 minutes	Time change offset is applied early.	Day of month calculation has been corrected.	All 4.2 supported platforms
M6220 - Simple mode, VLAN setting not active when move port to another group	Modular switch in Simple mode. Interfaces have VLAN settings different from default. If you move port from one aggregation group to another, VLAN settings are retained and are listed in running config but it is not active until system is rebooted or VLAN information removed and reentered again.	None – issue corrected	All 4.2 supported platforms
SSH configuration not restored after reboot	SSH config is not restored after reboot.	ssh configuration saved	All 4.2 supported platforms
PC8024 - VLAN trunk assignment CLI change	On 4.1.0.6 if VLANS are assigned to a trunk, the switch CLI will display the VLANS not assigned instead of the VLANS that are assigned	VLANs are displayed in positive format, i.e. assigned VLANs are displayed.	All 4.2 supported platforms
Web UI displays incorrect session timeout duration	After the browser session timeout (default 10 minutes), Web UI displays incorrect session timeout duration in the message "Your session had been inactive for more than 240 minutes	The displayed message was corrected.	All 4.2 supported platforms
PC8024 - Secure HTTP Random Characters - 4.1.0.6	If you go to system management, Secure HTTP, you will see random characters populating the fields. Even if you delete these entries and re-populate with valid chars, it will repopulate with invalid characters making it impossible to generate a cert using the web interface.	The random character rendering has been corrected.	All 4.2 supported platforms
Upgrades to 4.1.0.9 are causing network outages. The wizard from 4.1.0.9 fails to setup interfaces	The wizard in 4.1.0.9 fails to create any or very few interfaces and there was no config for any or very few of the ports, thus, the ip, icmp traffic was not working between ports as well.	Issue with switch upgrade has been resolved.	All 4.2 supported platforms

PC6220M GUI shows stack-ports down but CLI does not. In previous version issue didn't exist	The issue using CLI stack ports shows up and counters shows no transfer rate but GUI shows stack ports down.	Web shows stack ports up if they are up	All 4.2 supported platforms
M6220 - Routing fails on VLAN	Customer has multiple M6220 switches, and as part of a network change they wanted to remove a VLAN routing interface that was no longer in use. When they removed the IP address from this VLAN, they lost routing across the entire switch.	Ports are now checked to ensure they are not part of other routing VLANs before clearing the ARP policy on the port.	All 4.2 supported platforms
MIB walk crashes switch	SNMP MIB walk crashes switch.	A large array is allocated statically instead of on the stack.	All 4.2 supported platforms
M8024 - No password min length error using web GUI	On the web GUI-->system-->management security-->password management, If the password min length is unchecked and applied, there is an entry in the running config for "no passwords min-length". This can be verified through CLI. After this, on enable passwords page if we try to set a password which is any length less than 8, we get an error message as shown in the attachment.	Password ranges are now allocated dynamically on web pages.	All 4.2 supported platforms
Bug in Simple Switch GUI.	Once you select the Tagged-Vlans, there is NO way to unselect them again via GUI. Using command-line configuration is the only way to unselect those.	Tagged VLANs can be unchecked in simple mode	All 4.2 supported platforms
M6348 simple mode issue with 10G ports in aggregator group	Can't remove what running config says is there	Add interface command is corrected.	All 4.2 supported platforms
Banner motd configuration changes after reload.	The "banner motd" configuration changes after a switch reload.	Previously, the input mechanism ignored ANY lines beginning with an exclamation point. Now, the CLI engine will allow lines with a leading “!” in the banner	All 4.2 supported platforms
Error message via Web UI refers to "Management VLAN"	Attempting to assign an ACL to VLAN 1, via Web UI, generates an error message referring to the Management VLAN. "Error! Cannot Bind ACLs to Management VLAN."	the hard coded value has been removed in favor of the correct VLAN value	All 4.2 supported platforms
Web UI not generating error for out bound ACL & applies the config.	Binding an IP ACL as out bound to an interface, via Web UI, does not generate an error message. Furthermore, the config gets applied to the interface as an inbound ACL. When the same action is done via CLI, an error message is generated and the config is not applied.	Use of the direction object has been corrected.	All 4.2 supported platforms

Auto-neg option via Web UI is not grayed out for 10Gb fiber ports.	Auto-neg is an option in the port configuration via Web UI for 10Gb fiber ports. Ideally the auto-neg option should be grayed out for 10Gb fiber ports.	Auto-negotiation selection is disabled for 10G ports in the Web as auto-negotiation must always be enabled.	All 4.2 supported platforms
CLI command "show interface detail port-channel1" locks up console session	The CLI command “show interface detail port-channel1” generates the following errors: Max number of lines in the scroll buffer reached. Output will be truncated.	The scrolling issue has been corrected.	All 4.2 supported platforms
Creating VLANs, assigning ports using vlan membership detail page causes removal from running-config	Using web GUI to create and assign ports via vlan membership detail page causes previous vlan ports and sometimes previous vlan to be removed from running-config.	VLAN creation addition/removal behavior is corrected.	All 4.2 supported platforms
Assigning ACL Priority to a VLAN interface does not get set via Web UI	When binding an ACL to a VLAN interface, via Web UI, the "Assign ACL Priority" field does not get set as it would if it were configured via CLI.	Web interface has been corrected.	All 4.2 supported platforms
Incorrect Model numbers and revision date in dellref.my	The last revision date has not been revised. This could lead a customer to believe they do not need to update their MIB file. LAST-UPDATED "200311210000Z" -- 21 Nov 2003 12:00:00	The MIB has been corrected. Administrators are advised to load the new MIBs when updating to this release.	All 4.2 supported platforms
Links do not show status	Link dependency CLI "show link-dependency" shows "Member ports" and "Ports depended on" port numbers along with group id, but does not show the status of the members or the depended-on ports.	The display has been updated to show the requested information	All 4.2 supported platforms
M8024 does not save complete MST vlan configuration	Show spanning-tree mst-config not working.	All MSTP configurations are now saved.	PCM8024
Need to increase the VRRP routing instances or VRID to greater than 50	Previous limit was 20.	VRRP instances are now set to 50.	All 4.2 supported platforms
On the 8024F, inserting or removing the cable on ports 1 and 2 causes both ports to shut down briefly	The PowerConnect 8024F ports 1 and 2 will flap briefly when cables are removed and reinserted.	All inter-phy operation is fixed.	PC8024F

The CLI command terminal length is not setting terminal length value	When executing the command terminal length <value>, the value is not updated after execution.	Terminal length settings now take effect immediately.	All 4.2 supported platforms
The Service tag is being deleted on modular platforms.	When executing the “show system id” is not showing the service tag on modular platforms.	The service tag was accidentally being deleted and is now being saved correctly.	All 4.2 modular platforms.

Release 4.1.1.9

Summary	User Impact	Resolution	Affected Platforms
PC7048R-RA switch has boxes req cpu process 38-54% utilization with single power supply.	PC7048R-RA switch has cpu process boxes req running between 38-54 % utilization if it’s running either only with primary or secondary power supply.	Corrected CPU utilization issue when running with one power supply.	PC7048R-RA
Router crashes on OSPF network type change.	The switch can crash when changing the configuration from the default of broadcast to point-to-point.	Corrected process synchronization problem	All Platforms
Occasional crash when configuring VRRP.	With routing globally disabled, bouncing VRRP on a host interface occasionally causes a crash.	Correct the transition between routing being disabled and routing being enabled.	All Platforms
Cannot create Dynamic LAG with Interface range command	Dynamic LAG cannot be created from CLI using interface range command.	Correct the command syntax to "auto " instead of "active"	All Platforms
PC8024 cannot forward packets on port9 to port16 while linked on at 100Mb.	PC8024 cannot forward packets on port9 to port16 while linked on at 100Mb.	Correct interoperability problem between the PHY and the switching core.	PC8024 PC8024F
Show fiber-ports optical-transceiver is not displaying the correct interface numbers.	Instead of reporting on exact ports that had modules, diagnostics were reported on the ports that did not have modules	Corrected register problem when accessing the SPF+ ports	PCM8024
VRRP routing instances increased to 50.	VRRP routing instances increased to 50.	Increased VRRP routing instances table.	All Platforms
DHCP on in-band and out of band ports	The warning message about IP address conflict is not printed in case DHCP is configured on in-band and out-band ports and they both receive an IP address from one subnet.	Add warning message in case offered IP address is conflicting with the configured one on another port	All Platforms
Config commands did not migrate correctly from version 3.1.5.13	Command "spanning-tree mode mstp" doesn't migrate correctly from version 3.1.5.13.	Correct the command tree to migrate the old syntax.	All Platforms
Auto-neg option via Web UI is not grayed out for 10Gb fiber ports.	Auto-neg option via Web UI is not grayed out for 10Gb fiber ports for the PCM8024-k.	Corrected the Web UI.	PCM8024-k
Simple mode, VLAN setting not active when a port is moved to another group	if a port is moved from one aggregation group to other, VLAN settings are retained but not applied until reboot.	Correct initialization when port is moved.	PCM6220
Unable to configure secure SSH from web interface.	Error message 'sshcfg_load start' missing is returned.	Corrected Web page error.	All Platforms
Secure HTTP Random Characters	Random characters populate the Secure HTTP web page.	Corrected Web page data initialization.	All Platforms

Summary	User Impact	Resolution	Affected Platforms
IP PIMSM BSR/RP Mapping is not robust	When the RP or the BSR changes, the data traffic may get affected and in some case get software forwarded.	Corrected RP join processing.	All Platforms
Error messages when issuing a show statistics command while traffic running.	Accessing unsupported counters causes error messages to be displayed.	Change the logging priority of the messages for unsupported counters so that they are not output.	All Platforms
PCM6348 - Log message output	SNMP walk through unsupported counters cause error messages	Change the logging priority of the messages for unsupported counters so that they are not output.	All Platforms
Missing port VLAN membership in the GUI.	If switch has less than 24 ports, Port VLAN membership will not be shown in the GUI.	Corrected the VLAN port data issue.	PC70xx
Routing fails on VLAN.	Removing a VLAN routing interface causes routing to be lost across the entire switch.	Corrected the VLAN interface removal problem	PCM6220
PIM BSR join messages.	PIM Join messages using wrong RP Address	Corrected Join without a Prune condition.	All Platforms
PIM-SM Not all data passed down to the RPT.	When network re-configuration happens, the multicast traffic may not properly converge thus resulting in loss of some traffic.	Corrected Join condition.	All platforms
Port Configuration page gets errors on 10GB ports when any setting is changed.	Port Configuration page gets errors on 10GB ports when any setting is changed.	Corrected Web page error.	All Platforms
PIM-SM RP Fails to send Register Stops.	Register-Stop messages may not be sent out on the correct interface through to the First Hop Router.	Corrected Register Stops message error.	All Platforms
IGMPv3 querier sent in error with source address 0.0.0.0	Switch will get moved to non-querier mode if an IGMP membership query arrives with source address 0.0.0.0.	Corrected valid address check for membership query packet.	All Platforms
PIM-SM Joining messages using wrong RP address	PIM-SM Joining messages using wrong RP address	Corrected Join message processing.	All Platforms
Fails to reconfigure and forward multicast message	Switch fails to reconfigure and forward multicast messages following link failure	Correct an RPF information problem when link goes down.	All Platforms
DNS client error in logs and switch locks up and needs to be rebooted.	Error message “DNS Client: osapiSocketRecvFrom returned error for address 0xAABBCCDD” being logged	Corrected error in task that handles changes of the Service Port link status	All Platforms
PIM-DM Prune states expiring.	The router might end up sending Graft messages even though there are no intended hosts.	Corrected a PIM-DM timeout error.	All Platforms
Email alerts do not contain log message.	Current e-mail messages display in e-mail applications with a blank body, log message is not displayed.	Corrected error in email header section.	All Platforms
log message "internal interface number 183 out of range" is seen.	Message: “nimCheckIfNumber: internal interface number 183 out of range” is displayed.	Corrected error in VLAN create web page	All Platforms

Summary	User Impact	Resolution	Affected Platforms
"no enable authentication" does not disable access to privileged EXEC over the telnet line	"no enable authentication" does not disable access to privileged EXEC over the telnet line	Corrected error in authentication processing.	All Platforms
dot1q_api.c error during MIB walk	If LAG port is configured as general trunk then log message is getting printed when snmpwalk is accessing the MIB OID agentLagSummaryAccessVlanID.	Corrected VLAN access error.	All Platforms
sFlow Timeout settings for CLI command	sFlow receiver timeout value should be optional	Changed receiver timeout value to be optional.	All Platforms
sFlow: Limit of 32 for the number of interfaces for which sFlow can be enabled	Current limit of 32 for the number of interfaces for which sFlow can be enabled.	Changed the limit to allow all sFlow instances.	All Platforms
sFlow: Formatting errors with some of the records	Some of the sFlow records had formatting errors.	Corrected sFlow header problems.	All Platforms
sFlow: The sample Pool field is not being incremented properly	Sample pool field will not be incremented in the sFlow packet sent to the collector.	Corrected sample pool field error.	All Platforms
sFlow: The sFlow agent field isn't being filled in	The sFlow agent field isn't being filled into sFlow Packet.	Corrected problem adding sFlow agent address.	All Platforms
Stack module inserted in Bay 1 and SFP+ module in Bay 2	With the presence of stack module at bay1, SFP+ module in bay2 will not get detected until the stack-module at bay1 is removed.	Corrected error that prevented the detecting of SFP+ module in bay 2.	PCM6220
CLI "switchport general acceptable-frame-type" different options than GUI	The CLI "switchport general acceptable-frame-type" contains different options than GUI.	Options are now the same.	All Platforms
startup-config cannot be restored via tftp	TFTP script download or saved script validation will leave the DUT in an unusable state.	Corrected script validation problem.	All Platforms
"show ip ospf database" does not respect configuration of "terminal length 0"	The CLI handler of the "show ip ospf database" command does not consider the terminal length configuration.	Corrected terminal length configuration handling.	All Platforms
Occasionally, "clear config" from console triggers wio_api.c traceback	Occasionally, "clear config" from console triggers wio_api.c traceback	Corrected “clear config” internal message error.	All Platforms
Radius config stops working after reboot.	Radius config stops working after reboot, needs to be removed and re-added in order to work again.	Corrected error in Radius user authentication processing.	All Platforms
ISDP timers running fast.	ISDP entries are timing out and dropping off the list before the next update comes in.	Corrected an error in the ISDP timer disable processing.	All Platforms
VRRP hang	VRRP loss of mastership causes the switch to hang.	Corrected an error in the VRRP processing of the new IP address.	All Platforms
IPMC error messages and forwarding issue.	Error messages indicating that IPMC table are not set correctly in hardware.	Corrected error message processing which generated false error messages.	All Platforms
Dynamic LAG Ports are flapping/continuous trace messages.	Lags do not stay up on combo ports.	Corrected an error in mapping the physical ports to a LACP logical port.	All Platforms
Simple Switch should have FC enabled by default	Enable Flowcontrol on simple mode.	Flowcontrol enabled on simple mode.	All Platforms

Summary	User Impact	Resolution	Affected Platforms
Need to change message on console when try to downgrade anything below 4.1.0.19 release for new DDR	If a switch contains new DDR, downgrading to 4.1.0.19 is not allowed.	Modified the downgrade message.	PCM8024 PCM8024-k (with new DDR)

Release 4.1.0.19

Summary	User Impact	Resolution	Affected Platforms
Combo ports flapping when fiber port connected to certain other vendor switches	Users unable to reliably operate over combo ports	Corrected combo port flapping issue with new PHY firmware. Added new media-type command to configure the preference on a combo port	PC8024 PC8024F
New M8024/M8024-k cards have different memory parts requiring changes to DDR timings	User unable to downgrade to earlier version of firmware	No resolution. Newer IOMs do not support earlier versions of firmware.	PCM8024 PCM8024-k
10GBaseT ports do not come up	Unable to use 10GBaseT ports on PC7048R-RA	Corrected internal addressing of port. Ports now come up properly.	PC7048R-RA
Switch crashes when executing “show interfaces detail te1/2/1” command with no space between “te” and the unit/slot/port identifier	Service interruption due to crash	Issue has been corrected.	M8024 M6220 M6348 M8024-k
OOB Default Gateway does not save when using CLI setup wizard	There was no way to configure the gateway on Out-Of-Band interface.	Add functionality for configuring gateway on Out-Of-Band interface.	All Platforms
Upgrades to 4.1.0.6 are causing network outages. The wizard from 4.1.0.6 fails to setup interfaces	Ports on some devices will not attach.	Corrected the Configuration Wizard to properly apply the configuration to all ports.	All Platforms
The combo port is not coming up after performing repeated plug-out and plug-in.	The fibers port associated with Fiber / RJ45 combo ports may flap or not link up with certain other switches.	Add commands to allow operator to prefer or force RJ45 or SFP port selection on combo ports.	PC8024F/ PC8024
Line "no passive-interface Vl32" in startup-config does not get loaded on startup.	The "no passive-interface Vl32" configuration does not get loaded from the startup-config on startup.	Corrected the loading of the "no passive-interface Vl32" configuration.	All Platforms
Unable to configure Secure Shell from web interface.	Proper web page operation is prevented.	Web page has been corrected.	All Platforms
OpenManage web interface fails to provide an iSCSI web page when selecting the iSCSI item.	The web page for iSCSI fails to open when selected with OpenManage.	Web page has been corrected.	All Platforms
Wrong information for current link status in port configuration page.	Incorrect stacking link status is presented in the Web page.	Web page output has been corrected.	PCM6220

Summary	User Impact	Resolution	Affected Platforms
PFC sends packet after quanta extension received.	This can cause FCOE failures when using PCM8024-k as a transit switch between some switches.	Switch no longer sends packet after quanta extension received.	PCM8024-k
CLI command "show ipv6 interface" does not paginate correctly.	A large number of interfaces cause information to scroll off the viewing area.	Fixed the pagination for the command.	All Platforms
MOTD Banner appears at the wrong time.	MOTD and Login Banner is not visible before login for SSH users.	Fixed the banner processing function.	PCM6220
Summertime function running early.	The summertime function resets the time on the wrong week.	Corrected the function that returns the day of the week to account for particular months and leap years.	All Platforms
Switch does not save complete MST VLAN configuration.	The correct configuration was not being saved if there are more than 1K VLANs in a single MST instance.	Corrected the VLAN configuration buffer size.	PC8024 PCM8024
Switch failed to generate new RSA/DSA crypto keys.	“Failed to generate RSA key.” message was produced and keys were not generated.	Fixed error condition when generating keys.	PCM8024
Banner MOTD configuration changes after reload.	After reload a MOTD with an embedded! Character will be truncated.	Fix the MOTD engine to not ignore the leading ‘!’ character.	PCM8024
VLANs can get removed from running-config.	Creating vlans, assigning ports using the vlan membership detail page causes removal from running-config.	Corrected default VLAN checks when updating VLAN information.	All Platforms
Console session locks up.	CLI command "show interface detail port-channel1" locks up console session.	Corrected buffer overflow during "show interfaces detail" execution.	All Platforms
Fiber diagnostics reporting incorrect port type.	When running fiber diagnostics, Ports 5, 7, 8, 13, 15, 16 report to be fiber ports and not copper ports.	Fixed reporting of valid copper ports.	PC8024
BROADCOM-REF-MIB reporting incorrect values.	Incorrect Model numbers and revision date in BROADCOM-REF-MIB dellref.my	Model numbers which are described in dellref.my are corrected.	PC70XX
Switch crashes when full vlan range assigned to MST regions.	When the full range of VLAN instances is assigned to a MST region the switch crashes.	Corrected VLAN instance buffer overflow.	PCM6220
Config Wizard causes iSCSI error messages.	Using the config wizard to setup the PC8024 causes iSCSI error messages.	Correct the handling of iSCSI admin mode.	PC8024
SSH configuration not restored after reboot.	The 'ip ssh protocol 2' is not being included in the running configuration.	Corrected the ability to place 'ip ssh protocol 2' in the running-config.	All Platforms
1GB link being negotiated on 10GB Intel X520-KX4	Some internal links on the Modular switches will not link at 10Gb.	Corrected the port mapping to allow proper port configuration.	PCM8024 PCM8024-k
No message logged for "Max number of SSH login sessions exceeded"	When the Max number of SSH sessions is reached no error is logged.	Added an error message.	All Platforms
VLAN web page not updating.	When VLANs are removed using the web, the GUI doesn’t display the ports that are members of the VLAN.	Corrected the fetch of current VLAN data.	All Platforms

Summary	User Impact	Resolution	Affected Platforms
No password min length error when using web GUI.	If "no passwords min-length" Is set an error results if the password is less than 8 characters.	Correct password length range check.	All Platforms
MIB walk crashes switch.	When running a large SNMP MIB walk the switch crashes.	Corrected a memory problem in the MIB walk.	All Platforms
Unable to deselect VLAN tags in web GUI.	Once Tagged-Vlans are selected there is no way to unselect them again via the web GUI.	Corrected the Web page that allows tagged VLANs to be unselected.	PCM8024 PCM8024-k
Access is allowed to files on the switch without log in permissions required	If the file name is known, the file can be downloaded through the web browser without having to be logged in.	Corrected the web process to require login credentials before downloading a file.	All Platforms
Switch crashes when downloading without the .stk extension.	Switch crashes when trying to download code without .stk extension through HTTPS using HTTP.	Corrected download web page.	All Platforms
Switch crashing when HTTPS session is enabled.	Switch is crashing when HTTPS session is enabled from CLI but not from WEB	Corrected task table memory size.	All Platforms
Switch crashing when trying to open more than 3 HTTPS sessions	Opening more than 3 or more HTTPS sessions will crash the switch.	Corrected task table memory size.	All Platforms
Mozilla Java Script error when selecting VLANs.	In Mozilla, when 1-4085 VLANs are *selected* in the web page for Tagged VLAN Java Script error appears.	Corrected the code looping error.	All Platforms
IE7 error when selecting VLANs.	In IE7, when 1-4085 VLANs are *selected* in the web page for Tagged VLAN IE7 error appears.	Corrected the code looping error.	All Platforms
SDRAM test does not run the specified number of iterations.	When running the SDRAM test a <cntl-c> must be used to exit the test.	Correct the SDRAM test iteration loop.	PCM8024-k
PCM8024-k Web page and help page mismatch.	The help page for the PCM8024-k Switching--> Network Security--> Dot1x Authentication--> Authentication Detail page did not match the page.	Corrected the help page.	PCM8024-k
VPD CRC check hang	When the switch boots, If the CRC check of the VPD fails, the switch will hang.	Corrected check for valid VPD before CRC check.	All Platforms
Packet Buffer Optimization.	Improved Performance with High Utilization iSCSI Workloads.	Improved performance.	PC70XX PCM8024 PCM8024-k PC8024 PC6348
PCM6220 Stack View needs PCM70XX styling	PCM6220 Web pages did not have the same styling as PC70xx.	Updated the PCM6220 web pages.	PCM6220

Release 4.1.0.6

Summary	User Impact	Resolution	Affected Platforms
SSH crash - memPartAlloc: block too big	Reduced switch functionality.	Memory allocation issue is corrected and checked for memory leaks	All Platforms

Summary	User Impact	Resolution	Affected Platforms
PC M8024 switch reset out-of-band address to none when switchports were changed	Inability to access switches via OOB port.	The out-of-band address is maintained over switchport changes.	PCM8024
Web page shows IP address as '0.0.0.0' for '1.1.1.1' routing interface.	Potential operator confusion over switch operations	The web page output has been corrected.	All Platforms
Read-Only Web page is populating all configured IP and IPv6 ACL names when we select the ACL Name.	Potential operator confusion regarding web page operations.	The web page has been corrected to only populate the selected entry.	All Platforms
FAN LED graphic on web page needs to glow in RED when FANs are not operational (stopped).	Inability to determine switch status.	Web page has been corrected	All Platforms
Incorrect command is being displayed in running-config, when boot host dhcp is disabled.	Potential operator confusion regarding web page operations.	The running config now shows the correct configuration	All Platforms
DUT crashes while configuring max dynamic VLANs.	Network outage possible.	The PowerConnect does not crash when using maximum dynamic VLANs	All Platforms
Manager of the stack is changing when trying to learn maximum number of VLANs using GVRP.	Potential operator confusion regarding switch operations.	The stack manager does not change during learning with GVRP	All Platforms
Switch prompts to save config data when no changes have been made	Potential operator confusion regarding switch operation.	The switch no longer prompts to save config data if no changes have been made	All Platforms
Crash while RFC3918 Group Capacity test is running	Network outage possible.	The PowerConnect switch runs the RFC3918 test without crashing	All Platforms
'no' version of 'key' command is not implemented	Potential operator frustration with switch management.	The **no key** command is implemented to return the key configuration to the default.	All Platforms
Password is not accepting quotation (") character	Potential operator confusion regarding switch configuration.	Passwords can be enclosed in quotes (contain embedded blanks). A password may not contain a quote. The accepted character set and length is documented in the CLI reference manual.	All Platforms
Incorrect warning message displayed while executing the command "boot system <unit> image1"	Potential operator confusion regarding switch operation.	The error message has been corrected to indicate that the unit selected for reboot does not exist.	All Platforms
IPV6 command displays wrong output	Potential operator confusion regarding switch operation.	The IPv6 output has been corrected to remove the duplicate display lines in **show ipv6 help.**	All Platforms
LLDP-MED log messages showing 5 sec difference in entry age out information	Potential operator confusion regarding switch operation.	The LLDP timer has been updated to account for processing skew.	All Platforms

Summary	User Impact	Resolution	Affected Platforms
DHCPv6 web issues	Potential operator confusion regarding switch configuration.	The acceptable character sets are documented in the CLI Reference guide.	All Platforms
LLDP MED application should not allow configuration of location and inventory transmit TLV's as underlying application not present	Potential operator confusion regarding switch configuration.	Location and inventory TLVs cannot be enabled for transmission in LLDP MED.	All Platforms
SysUpTime is not being shown correctly during an SNMP walk (Poll interval 1sec)	Potential operator confusion regarding switch operation.	The correct variable is used to write SysUpTime	All Platforms
Log messages need to be corrected on ip dhcp snooping rate limit scenario.	Potential operator confusion regarding switch configuration. Inability to diagnose network issues.	Interface representations in log messages use unit-slot-port format.	All Platforms
The **show ip vlan** command output is not proper after more-quit prompt is encountered, i.e. after around 16 routing interfaces	Potential operator confusion regarding switch configuration.	The paging has been corrected.	All Platforms
Invalid error port number displayed on log message when vlan is changed to forbidden mode from access mode	Potential operator confusion regarding switch configuration.	The error message is no longer issued.	All Platforms
The **banner motd XXXXX** does not appear in show running-config	Potential operator confusion regarding switch configuration.	All banner configuration appear in the running-config	PCM8024
Web page mac-vlan table too slow to load.	Potential operator frustration with switch management.	For certain browsers, paging has been implemented to speed up load times.	All Platforms
Confused between **ip default gateway** and **ip default route** (update manual with how to set a default route).	Potential operator confusion regarding switch configuration.	The ip default route command is deprecated. Use the **ip default route** command to set a default route.	All Platforms
Auto Install **show boot retry** count line needs to be left aligned by one space.	None.	The retry count alignment is corrected	All Platforms
Cannot Access Optical Transceiver Diagnostics Page if Multiple Submits done prior to initial refresh completing	Potential operator frustration with switch management.	This is a browser dependent issue (IE 6) that is not seen in later versions. The web session recovers after doing a refresh.	All Platforms
Error messages for non-existent stack members non-informative	Potential operator confusion regarding switch configuration.	The user can pre-configure stack units. If the stack unit does not exist for a switch configuration operation, an error message indicating same is issued.	PC70XX

Summary	User Impact	Resolution	Affected Platforms
Traffic is forwarding when IPv6 forwarding is disabled	Incorrect operational state in network.	The ipv6 forwarding command is deprecated. To disable traffic forwarding, use the "**no ipv6 unicast-routing"** in place of the "**no ipv6 forwarding"** command.	PCM8024
A LAG member comes UP if configured individually as no shutdown, even though the port-channel's state is down	Incorrect operational state in network.	LAG members are placed in the blocking state for dynamic LAGs and only come up when the LAG link comes up.	All Platforms
Re-authenticate Now check box is not highlighted when edit check box is selected	Inability to configure switch.	The Re-authenticate Now check box is highlighted when the edit check box is selected	All Platforms
Block command is not seen in show running config through web and cli	Potential operator confusion over switch operations.	The block command is a temporary administrative assignment and is not maintained persistently in the saved or running configs.	All Platforms
FDB entries are getting aged out before default age-out time, when both FDB and MFDB tables are full.	Potential operator confusion over switch operations.	On the PCM6220, the MFDB and FDB tables are a shared resource. The user is continually sending new MFDB entries, which causes old FDB entries to be removed to make a place for the new MFDB entries.	All Platforms
DHCP packets forwarding is not proper to/from the trusted and un-trusted ports	Incorrect operational state in network.	The frame flooding routing in DHCP snooping now takes into account trust status.	All Platforms
Configuring all ports in all VLANs takes a long time	Potential operator frustration with switch management.	VLAN configuration has been optimized.	All Platforms
Max number of OSPF neighbors not supported	Potential operator confusion over switch operations.	The maximum number of neighbors is supported.	All Platforms
Cable fault distance not getting displayed in WEB in case of cable with one or more pairs cut or short.	Potential operator confusion over switch operations.	The fault distance is displayed in the web page.	All Platforms
Ports representation need to be changed in debug messages	Potential operator confusion over switch operations. Inability to diagnose network issues.	Ports are now displayed in C/S/P standard format	All Platforms
No error message for illegal characters in various command parameters	Potential operator confusion over switch configuration.	The accepted character set and length is documented in the CLI reference manual.	All Platforms
The ARP entry is not seen in the ARP table when an ARP reply is sent to DUT.	Potential operator confusion over switch operations. Inability to diagnose network issues.	ARP entries are stored properly	All Platforms
Mapping Table configuration is not being displayed on Read-Only mode user web page.	Potential operator confusion over switch configuration.	The mapping table is displayed for a read-only user.	All Platforms
ACL is getting deleted when trying to create max+1 rule.	Potential operator confusion over switch operations. Possible security issues.	Corrected error checking logic.	All Platforms

Summary	User Impact	Resolution	Affected Platforms
LLDP-Med TLV information not registered for jumbo frame sizes greater than 8000	Potential operator confusion over switch operations.	Jumbo LLDP frames are now processed properly	All Platforms
VLAN binding entries are not being displayed on Read-Only mode user web page.	Potential operator confusion over switch operations.	VLAN binding entries are available to read only users	All Platforms
Unable to execute the command dot1x timeout tx-period 1	Potential operator confusion over switch operations.	This command is accepted with a timeout period of 1 second. Corrected range check on input.	All Platforms
In switching> network security >dot1x authentication web page in read-only user mode, the Re-Authenticate Now check box can be checked	Potential operator confusion over switch operations. Possible security issue.	Read-only properties are set for the check box	All Platforms
System Device information web page LED information not in sync with front panel LED information.	No Potential operator impact expected.	This issue was regarding various stylistic aspects of the system device web page. The system device web page conforms to the requirements as it exists and does necessarily match the CLI with regarding to capitalization or naming conventions	All Platforms
DHCP snooping static binding thru DHCP request is denied as this is an expected behavior.	Potential operator confusion over switch operations.	Removed the log message indicating that a bound DHCP client with an existing binding sent a DISCOVER. Added a counter for this condition to the DHCP debug statistics.	All Platforms
Mode of transfer is displaying “unknown,” while downloading the code from ftp	Potential operator confusion over switch operations.	ftp transfer mode is displayed	All Platforms
Allow disabling and enabling of terminal paging	Potential operator frustration over switch configuration.	The terminal length command is now implemented.	All Platforms
Web does not allow to configure image descriptor to its max length i.e. 255 characters.	Potential operator confusion over switch operations.	Images descriptors up to 255 characters are allowed	All Platforms
CDP (ISDP) is active on port-channels instead of the member Ethernet interfaces. For dynamic LAGS, the ISDP information is not exchanged on the interface until the port-channel becomes active.	Potential operator confusion over switch operations. Inability to interoperate with other switches.	CDP is active on the member ports for dynamic LAGs when the LAG is active.	All Platforms
CLI Manual Has No Index	Potential operator frustration over switch configuration.	The CLI manual has an index.	All Platforms

Summary	User Impact	Resolution	Affected Platforms
Script validation is fails when max SNTP servers are configured.	Potential operator confusion over switch configuration.	Corrected CLI validation check so that existing server can be entered multiple times.	All Platforms
Configured SYSLOG server parameters cannot be updated without deleting and re-configuring	Potential operator frustration over switch configuration.	Syslog server parameter can be updated in the CLI without deleting the server.	All Platforms
CLI will not let user configure available parameter for the given IGMP command	Potential operator frustration over switch configuration.	IGMP configuration commands can be entered in interface VLAN mode at any time.	All Platforms
Inconsistent behavior - using same port number for multiple services	Potential operator confusion over switch operations.	Attempting to add a service with a TCP port overlapping a TCP port used by an existing service is denied with an appropriate error message.	All Platforms
LLDP Assignment of port ID for Port-Description TLV	Potential operator confusion over switch operations. Inability to diagnose network issues.	The LLDP port id TLV is supported by PowerConnect and can be displayed on peer devices.	All Platforms
Management ACL list needs "Match every packet" option	Potential operator frustration over switch configuration. Possible security issue.	New syntax has been added to the management ACL to allow the **any** specification for the service type.	All Platforms
SNMP support for Dell-LAN-TRAP-MIB	Potential operator frustration over switch configuration.	The Dell-LAN-TRAP-MIB is supported.	All Platforms
Simple mode BPDU will pass thru port-aggregator to other port-aggregator when using a single link per aggregator	Network outage if connected to Cisco with BPDU-Guard enabled	BPDU flooding is now disabled on aggregator ports.	All Platforms
Fatal error crash and reload when uplinked to Cisco 6509 - 3.1.3.9 - Believe to be ISDP	Inability to connect to Cisco 6509 CDP enabled ports	The switch now handles CDP mega-packets of size 1376.	PCM6220
Interface metric not working on 8024 OSPF passive interface	Interface metric is advertised as 0 when configured as passive – passive interface preferred over active interface	The interface metric is advertised properly when the interfaces is configured in passive mode.	All Platforms
Local system MAC address displayed as partner MAC address in "show lacp port-channel"	Potential operator confusion over network topology	The partner MAC address is displayed in the Partner system MAC address field.	All Platforms
SNMP going unresponsive on modular switches within 6 hours	Potential operator frustration over switch operations	SNMP operations have been corrected and tested without issue for over 24 hours.	All Platforms
Network performance and connectivity issues. Evidenced by “l7utils_inet_addr” messages in log.	Potential operator frustration over switch operations	The internal timer operations have been highly optimized resulting in lower overall CPU utilization.	All Platforms
H323 VoIP traffic and Crashing/Rebooting switch. CPU PID '17c31570 voipTask' spikes as seen in the 'show process cpu'.	Potential operator frustration over switch operations. Switch degradation in VoIP deployments.	The VOIP QOS code is no longer processing VoIP packets when it is admin disabled.	All Platforms

Summary	User Impact	Resolution	Affected Platforms
LACP not working with Juniper EX-4200, show inactive port channel state. System is sending oversize (132 bytes) LACP PDUs.	Potential operator frustration over switch operations. Inability to interoperate with Juniper switches.	The LACP process now sends 128 byte LACP PDUs. Interoperability with Juniper switches is verified.	All Platforms
Stack splits into multiple masters when MU fails.	Potential operator frustration over switch operations.	Issue in SDK MAC reset function resolved such that connected unit respond to master within 1 ms. Stacking stability verified under the conditions where issue occurred.	All Platforms
VLAN name issues in web UI on modular. Old VLAN name is retained on web page when switching to new VLAN.	Potential operator confusion over switch operations.	The correct VLAN name is always displayed.	All Platforms
Discards Occurring After Firmware Update to current version 3.1.5.4.	Potential operator confusion over switch operations.	The wrong counter was being displayed in the CLI. The CLI commands “show statistics port-channel” and “show statistics <interface>” are corrected to use the same counter as SNMP.	All Platforms
STP topology changes when an OOB SSH connection is established	Potential operator frustration over switch operations.	The SSHD task was starving other tasks in the system and causing topology changes. The SSHD task priority is now set to the shared time slice priority.	All Platforms
ARP broadcast traffic not forwarded through static/dynamic 10Gb LAGs	Potential operator frustration over switch operations. Potential network instability.	A field was being utilized in the LAG hash algorithm that could result in different hash indices on different units of a stack. This field (modid) has been removed from the hash selection algorithm.	All Platforms

CLI Reference Guide Updates

Release 5.1.0.1

The following table lists issues found in the CLI Reference Guide after publication:

Command	Issue
ip igmp snooping querier query-interval	The guideline under this command refers to the IGMP Snooping Max Response Time. A reference that this can be configured using command ip igmp query-max-response-time under IGMP commands is missing. The default IGMP/MLD snooping Max Response Time is 25 sec
terminal monitor	The command does not have any arguments or a particular expected output hence an example for this is missing in the guide. prompt#: terminal monitor (in privileged exec mode to display logging messages on terminal)
ip mtu	The guideline should be augmented with the below text: Use the ip mtu command in Interface Configuration mode to set the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Packets that are L2 forwarded in hardware ignore the IP MTU. Packets that are L3 (VLAN routing) forwarded in hardware observe the IP MTU. Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.
rate-limit cpu direction input pps *pps_value* **no rate-limit cpu direction input pps**	Use the rate-limit command to reduce the amount of unknown unicast/multicast packets forwarded to the CPU. Use the "no" form of the command to set the rate limit to the default value. pps_value – range 100-1024 packets per second (100-3000 for PC81xx switches). The default ingress rate limit is 1024 packets per second (3000 for PC81xx switches). This command allows the administrator to reduce the rate limit for which unknown unicast and multicast packets are forwarded and/or copied to the CPU. It does not affect the rate limits for control plane packets. It is almost never necessary to use this command to change from the default value. The use of this command should be restricted to situations in which moderate to high rates of unknown unicast/multicast are continually sent to the switch CPU as evidenced by the show proc cpu command and where the ipMapForwardingTask is showing high CPU usage. This will occur most frequently in networks where a high number of ARPs are continually received on untrusted ports, high numbers of L2 stations are timing out and reappearing or multicast flooding is occurring in the network. If problems with L2, L3 or multicast learning occur after changing this value, set the rate limit back to the default value and take other steps to correct or mitigate the underlying network issue directly. Note: This command is not available on the PCM6220 switch.
show system internal pktmgr internal control sw-rate-limit	The show command is to display the configured CPU rate limit for unknown packets in packets per second. Note: This command is not available on the PCM6220 switch.

Release 5.0.1.3

- No Updates

Release 5.0.0.4

Command	Issue
Show snmp filters Snmp-server filter	The following note should be added to the command usage guidelines. When a filter is defined, SNMP treats the filter as having an 'exclude all' statement at the beginning of the filter. Unless an include statement is specified, all notifications will be excluded.
aaa authorization {exec } {default | <list_name>} method1[method2] no aaa authorization {exec} { default|<list_name>} authorization exec [default |<list_name>] no authorization exec debug aaa authorization exec no debug aaa authorization exec	The following Exec Authorization CLI commands are missing from the CLI reference guide aaa authorization {exec } {default | <list_name>} method1[method2] no aaa authorization {exec} { default|<list_name>} authorization exec [default |<list_name>] no authorization exec debug aaa authorization exec no debug aaa authorization exec

Release 4.2.2.3

- No Updates

Release 4.2.1.3

Command	Issue
Storm-control broadcast	The supported syntax is **Storm-control broadcast [level *rate*]** where ***rate*** is a parameter to **level** and defined to be: The storm-control threshold as percent of port speed. Percent of port speed is converted to PacketsPerSecond based on 512 byte average packet size and applied to HW. If **level** is not used the default ***rate*** is 5.
name "RDU-NOC Management VLAN"	The VLAN name command has been migrated to VLAN Config mode and is no longer available in interface VLAN mode.

Release 4.2.0.4

- Please refer Dell PowerConnect CLI Reference Guide for more details

Release 4.1.1.9

- No Updates

Release 4.1.0.19

The following commands are supported on switches that have combo ports:

Command media-type

Syntax:
media-type { auto-select [rj45 | sfp] | rj45 | sfp }

auto-select rj45 - utilize RJ45 media when both media types are active
auto-select sfp - utilize the SFP media when both media types are active
auto-select – return the selection to the default (auto-select sfp)
rj45 – force connection on the RJ45 port. Power off SFP media port
sfp – force connection on the SFP port. Power off RJ45 media port

Default Configuration:
The default is “media-type auto-select sfp”

Command Mode:
Interface Config mode

Description:
Select the media type for the interface. This command is only valid on combo ports.

User Guidelines:
When both media types are connected, the preference as determined by the auto-select keyword parameter selects the active media. When the auto-select keyword is not specified, the selected media type is powered on and the alternate media type is powered off. Note that when the auto-select keyword is used with any media type, the SFP port will remain powered and the laser, if any, will remain on in order to allow connections over the SFP port.

Examples:

! Select the RJ45 port and power off the SFP port
console(config-if-Te1/0/24)#media-type rj45
! Prefer the RJ45 port and leave the SFP port powered on
console(config-if-Te1/0/24)#media-type auto-select rj45

Command show interfaces media-type

Syntax:
show interfaces media-type

Default Configuration:
N/A

Description:
Display the configured and active media type for the combo ports

User Guidelines:
N/A

Examples:

```
console#show interfaces media-type

Port       Configured Media-Type(s)     Active
---------  --------------------------   ------
Te1/0/21   auto-select, SFP preferred   SFP
Te1/0/22   auto-select, SFP preferred   SFP
Te1/0/23   auto-select, SFP preferred   Down
Te1/0/24   auto-select, SFP preferred   Down
```

Release 4.1.0.6

The Dell PowerConnect CLI Reference Guide is completely new. Users are referred to the Dell PowerConnect Configuration Migration White Paper for information on how to migrate configurations from previous releases of Dell PowerConnect firmware to the 4.0.0.6 Dell PowerConnect firmware.

The following table lists issues found in the CLI Reference Guide after publication:

Command	Issue
show service-policy in	The supported syntax is **show service-policy {in|out}**
show copper-ports cable-length	This command is deprecated. Use the **show copper-ports tdr** command to display the stored information regarding cable lengths and the **test copper-port tdr** command to perform a cable length test. Testing a port brings the port down momentarily.

User's Configuration Guide Updates

The following table lists issues found in the User's Configuration Guide after publication:

Release 5.1.0.1

Issue
The following paragraphs need to be added to the User's Guides for all platforms except the PCM6220: Unknown unicast and multicast packets are copied to the CPU on the lowest priority QoS queue. Unknown packets are those that do not have hardware forwarding entries. Known unicast/multicast packets are hardware forwarded and are not queued to the CPU. Control plane packets (e.g. spanning tree BPDUs) are copied or forwarded to the CPU on higher priority queues. The rate limiting for unknown packets occurs on the internal CPU port and does not affect hardware based traffic routing/forwarding in any way. Typically, the switch will examine the received packets in software to check if there is a forwarding entry, create a forwarding entry (e.g., add a L2 MAC address or ARP response), and then either discard the packet or software forward the packet (only occurs during the brief transitional period when the system is actively adding a hardware forwarding entry but the hardware is not yet updated). Processing delays for higher priority packets may occur when the internal CPU queue is continually kept busy handling low priority packets. A command was created to allow the administrator to reduce the rate limit for which unknown unicast and multicast packets are forwarded and/or copied to the CPU. It does not affect the rate limits for control plane packets. It is almost never necessary to use this command to change from the default value. The use of this command should be restricted to situations in which moderate to high rates of unknown unicast/multicast are continually sent to the switch CPU as evidenced by the show proc cpu command and where the ipMapForwardingTask is showing high CPU usage. This will occur most frequently in networks where a high number of ARPs are continually received on untrusted ports, high numbers of L2 stations are timing out and reappearing or multicast flooding is occurring in the network. If problems with L2, L3 or multicast learning occur after changing this value, set the rate limit back to the default value and take other steps to correct or mitigate the underlying network issue directly. See the CLI Reference Guide updates section of this document for the description of the "rate-limit cpu" CLI command and its use.

Release 5.0.1.3

- No Updates

Release 5.0.0.4

Issue
The following message needs to be added to warn the user that Hotplug of a module is not supported if one of the ports on the module is operating in stacking mode. *Warning: One of the modular ports is operating in stacking mode.* *Hotplug of a module requires system reboot.* *Failure to do so will make the system unstable!*
The following copper SFP needs to be listed as the supported module. However, diagnostics are not supported on copper SFP's. Finisar FCLF-8521-3
When a filter is defined, SNMP treats the filter as having an 'exclude all' statement at the beginning of the filter. Unless an include statement is specified, all notifications will be excluded.

Release 4.2.2.3

- No Updates

Release 4.2.1.3

- Please refer Dell PowerConnect Users Guide for more details

Release 4.2.0.4

- Please refer Dell PowerConnect Users Guide for more details

Release 4.1.1.9

- No Updates

Release 4.1.0.19

The default authentication profile has changed from "enableList" to "enableNetList:

Telnet and SSH default to using the enableNetList authentication profile which requires an enable or line password. The serial console defaults to using the enableList authentication profile which does not require the use of a password. This change increases compatibility with industry standard behaviors. In previous releases, telnet, SSH and the serial console defaulted to using the enableList profile which does not require a password.

The following table lists changes to the User's Configuration Guides after publication:

Change	Affected Platform
Added examples of how a user would implement VLAN or QoS policy assignment in the Port Based Security section.	All Platforms
Added a table of the RADIUS attributes supported by the PowerConnect switches in the Controlling Management Access section.	All Platforms
The valid VLAN range is described as 1 to 4093 (multiple sections)	PC70xx
A better description of the RADIUS 'deadtime' parameter is added to the Controlling Management Access section	All Platforms
The CLI command "monitor session 1 mode" is described in the Configuring Port Mirroring section	All Platforms

Known Issues

The following are all the outstanding known issues from previous releases. The issues listed here may have been discovered on any of the switches listed on the title page.

Release 5.1.0.1

Summary	User Impact	Workaround
Molex QSPF DAC Cable with part number 111040-1104 does not comply with QSFP specification SFF-8436. These cables do not support 'voltage' diagnostics.	Voltage is displayed as 0.00 instead of "N/A" for this diagnostic parameter.	Ignore the voltage displayed field for this part or use a SFF-8436 compliant cable.
Show AAA IAS-USERS <Username> Command Missing	The “show aaa ias-users [username]” command seems to have been deprecated even though it still exists in the CLI guide.	The same information can be seen within the running configuration of the switch with the “show running-config” command.
PC70xx - Email alerts fail when logging level is default	PowerConnect 7048 switches that are setup to send email alerts for log messages at the default level can produce the following log message: Email Send Failed! No of Email sends Failed So far= 328	Change the email logging level to something other than default, i.e. informational alerts. The switch will then send the alerts with no issues.
Web UI issues with pre-provisioned ports in stacked environment.	The Web UI seems to be saving the configuration for pre-provisioned ports but when the stack is reloaded the configuration for these ports are no longer correct.	Use the CLI if possible.
External CDP/ISDP traffic occasionally forwarded onto internal ports	Occasionally external CDP/ISDP packets are being forwarded to the internal ports. This results in confusing information from the blade server point of view as multiple directly connected neighbors appear to be seen.	None.
Multicast sources that cease sending multicast are timed out and removed from the multicast forwarding cache after 150 seconds	If an intermittent multicast source that has been aged out of the multicast forwarding cache begins sending again before the corresponding S,G entry has timed out at the RP (185 seconds per RFC 4601), any *,G entries (joined hosts) may take up to one IGMP Query interval to begin receiving the multicast stream.	The default IGMP query interval is 125 seconds. In practice, this situation is very unlikely to occur as a multicast source that fails to send even one packet for 150 seconds is unlikely to start sending packets before the S,G entry at the RP times out.

Release 5.0.1.3

Summary	User Impact	Workaround
ipv6 ping is not reliably working	IPv6 functionality requiring Neighbor Discovery will not work	None

Release 5.0.0.4

Summary	User Impact	Workaround
QSFP Base CR4 with copper DAC cable lengths greater than 3 meters will not work on PC8100 switches	When using the DAC copper cables with QSFP CR4s (which are rarely used) and cable more than 3 meters, the switch may not even detect this device and so link up never happens. Only the following cables are recommended with these CR4 QSFPs: 111040-1104 – 1m Passive Copper Assembly 111040-1204 – 3m Passive Copper Assembly	None
On PC8100 switches, sharp decrease in 6to4 tunnel traffic is observed when ipv4 static route is deleted and added back to the switch.	This is a corner case issue requiring many steps to get to this state but if the state is reached, the user will see less through-put on the tunnel.	Stop traffic for a minute or two so that the stale entry in the Linux stack is cleared.
Failure log messages may show up on console on doing a SNMP walk on root node.	There is no effect besides the annoyance of these messages while doing an SNMP walk.	None
Speed is not applied to combo (copper) ports after saving and reloading the DUT (8024/8024F).	Since these configuration variables exist for both copper and fiber modes (combo ports), the speed and duplex are not saved since the port assumes that it will only save fiber parameters and thus the customer will notice that the port auto-negotiates after reload instead of goes to a static speed or duplex.	Always reconfigure the speed on copper combo ports after reboots on the 8024/8024F.
SFP+ module is still detected in running-config after clear config on PC8100 with QSFP to 4x10G	The information that will be stored in the running-config specific to the 4x10G port (QSFP to 4x10G) will not be cleared after the clear config command.	User can negate these commands manually after a clear config.
Status is not shown after the image upload using HTTP through IPv4 HTTPS session	The user may not be aware that the download has completed when using the GUI.	User must refresh screen or go to version screen for indication that the download has completed.
Console logs/syslogs are not generated if we disable LAG local preference.	This will only be seen when disabling the local LAG config and will not affect the system.	None
The following unwanted logs may come up on console after running the “clear config” command. 1) dot1s helper logs 2) snooping logs 3) “ATP RX: Failed to alloc” logs	There is no effect to the switch or user, just unwanted log messages on console.	None

Summary	User Impact	Workaround
The following unwanted logs may come up on console after running the “show tech-support” command with UDLD and MSTP configured: “ATP RX: Failed to alloc” logs	There is no effect to the switch or user, just unwanted log messages on console.	None
On PC8100 switches, console gets locked for 20-30 seconds if trying to add a 6to4 tunnel source within 30 seconds of deleting another tunnel source.	This only happens after repeated attempts at adding and deleting a tunnel source and thus the impact is very small to the customer.	Wait for 30 seconds after deleting the tunnel source and then add a new tunnel source.
'out of mBlks' logs are observed on console if ICMPv6 echo requests are sent to OOB port at line rate	There is no effect to the switch or user, just unwanted log messages on console.	None.
Invalid characters are shown under reason column for some entries in the “show ip ospf statistics” command.	This only happens with this CLI command output and thus might be bothersome.	The Web interface will not show these characters.
LPI samples are not shown for the first time on selecting a different unit number using the GUI.	This can be confusing to the user since the switch will not show the stats for the port after a new unit is selected but then the stats will show up after going to new port and then back.	Select a random port from the web and then re-select the desired port to view the LPI samples.
"show fiber port optical-transceiver" command is showing current as zero for QSFP transceivers.	This field does not apply to QSFP transceivers and should display “NA” instead of zero.	None.
Image uploaded with HTTP method can't be downloaded back to the switch if switch and PC are located in different networks and the networks are very slow.	This might require the User to have to retry the download or change the IP address or VLANs on the switch or PC.	Use alternate transfer methods like TFTP, FTP, etc.
Console messages shows "Thermal state raised to WARNING" often.	Our customers requested this warning to indicate better visibility into the Thermal settings and sensors.	Configure the logging level to be higher than “Warning”.
Finisar LRM 10G SFP+ transceiver model – FTLX137D3BCL - drops packets intermittently.	This specific model is not recommended for use with our switches.	Please use the Avago 10G-BaseLRM model – AFBR-707SDZ-D1.
OpenManage displays incorrect session timeout duration	OpenManage timeout warning window is displaying the wrong value but uses the set value.	None.
Command "show fiber-ports optical-transceiver" causes UI to become slower with multiple transceiver count.	Executing the command “show fiber-ports optical-transceiver” with multiple transceivers inserted will cause the console prompt a long time to return (possibly up to 60 seconds).	None.

Summary	User Impact	Workaround
Port goes down if the port is excluded from native vlan with UDLD feature enabled on it.	If the port is operating in Trunk mode and UDLD is enabled, the port goes down if it is excluded from the native vlan.	Include the port in native vlan.
SNMP V3 walk may fail after “initiate failover” command is issued.	After failover, SNMP V3 walk may fail, as MIB browser and agent can become out of time and stop intercommunication.	After a failover, close the browser and re-open it. SNMPv2 works correctly.
OOB static IP entry cannot be the same as the DHCP assigned IP address	After receiving an IP address from the DHCP server, the switch gives an error and will not allow an attempt to add a static IP address and gateway that is the same as the DHCP IP address.	Use a different IP address than the DHCP address given.

Release 4.2.2.3

Summary	User Impact	Workaround
Stack member units port display is missing in web GUI.	Wrong id for the power LED is displayed.	None
WebUI sFlow Polling page issues.	sFlow>Sampler configuration and sFlow>Poll Configuration don't work for ports Gig1/0/1 - 1/0/9.	None

Release 4.2.1.3

Summary	User Impact	Workaround
"show interfaces switchport " command shows incorrect General Mode Tagged VLANs value	Some general mode VLANs tagged to the interface may not be displayed using this command.	Use “show vlan” command to interfaces. No other workaround.
M6220 OOB interface unreachable after failover	On a failover on a M6220 stack the OOB interface may not be available.	Recovers when the master is restored.
CLI command "show ip dhcp snooping binding" not displaying client information.	"show ip dhcp snooping binding" not displaying client information. "show ip dhcp snooping statistics" does not display correct message counts.	None
OOB interface configured with default IP via Setup Wizard though told not to do so.	The setup wizard does not honor selection to not setup OOB IP address.	OOB IP address will need to be setup manually.
DHCPv6 - M6220, PC/M 8024/k - Client Solicits do Not Seem to Make it to the Server / Relay	By looking at the counters, the client believes it is sending solicits; but, the relay and the server never see the solicitations.	None

Release 4.2.0.4

Summary	User Impact	Workaround
File modification date & time is not getting updated with current time & date.	When internal files are modified, they do not get the current time stamp.	None

Summary	User Impact	Workaround
SNMP walk is not successful while doing walk on root port.	SNMP walk on the root port times out.	Do not do SNMP walks using root port.
FIP sessions are getting disconnected for VLAN switchport mode change with default vlan settings.	Users are unlikely to change either the default VLAN or the FIP VLAN while sessions are active.	Do not change the FIP VLAN while sessions are established. The reason is that after a VLAN is re-assigned or even changed to general mode, the sessions will of course be disrupted since the FIP snooping occurs on the VLAN and any change in this will cause problems on the Cisco Nexus side and will require an interruption and reestablishment of the addressing from the CNAs on up.
OpenManage displays incorrect session timeout duration when using secure HTTP	After the browser session timeout (default 10 minutes), OpenManage displays incorrect session timeout duration in the message "Your session had been inactive for more than 240 minutes", which is the actual setting for telnet and ssh. However, the actual timeout occurs after the default period of 10 minutes, so the GUI message is incorrect.	Disregard the time in this GUI message.
Cannot disable the SFS "allow-downgrade" feature	Even with SFS allow-downgrade disabled, the master will still push the older firmware to a stack member running a newer version of code.	Always make sure the master has the wanted version loaded.
Console port locks up when awaiting telnet Radius response	Radius authenticated Telnet login attempt when Radius daemon stopped, causes console port to be temporarily blocked until Radius timeout expires.	Wait for timeout or ensure Radius server is reachable.
Flowcontrol is in inactive state when connected to Partner(Randall) with combo ports.	Flowcontrol gets automatically disabled and if the ports have a need for Flowcontrol, there will be no pause frames sent.	Re-enable Flowcontrol on Randall switch.
7048R replacement power supplies reported as incompatible	Although the power supplies part number is the same, the 7048R reports it as incompatible and thus the error message is incorrect. The power supplies still works correctly.	Ignore the error message, since there are no functional issues with this power supply.
PowerConnect 7048P : poe_lldp.c(1741) 23137 %% Failed to get pairs control	After a long period of time and numerous IP phones connected and with at least 5 switches connected as a stack, PoE error messages start filling the logs.	Maximum supported IP phones at this time is 64.
SNMP showing packets discarded while cli doesn't show the same.	SNMP monitoring tool is pulling stats from M8024 and shows very high discard receive rate but switch doesn't say the same.	None.
PC M6220 Running configuration altered after removal of stacking master, 4.1.0.19, 4.1.1.7	When master member was removed from and reinserted into an M1000e enclosure, some of the configuration was missing from running-config.	Always write the config before removing master.
Stacked m8024-k or 8024/8024F switches running code that supports Ethernet stacking should not be downgraded to older code that doesn’t support Ethernet stacking.	Customers downgrading a switch stack to a version of code that does not support stacking are advised to: 1) Break apart the stack into individual units 2) Clearing the saved config on each unit 3) Renumber each unit to unit 1 using the switch X renumber 1 command	Failure to follow these instructions may cause units to crash when booted into the 4.1 firmware. To recover the switch, attach a serial cable and enter the boot menu (press 2 - Start Boot Menu at the prompt). From the boot menu, select 10 - Restore configuration to factory defaults, and then select 1 - Start operational code

Summary	User Impact	Workaround
PC7048P, in a stack will error out when all rebooted at the same time.	The stack will stop passing traffic if all switches in the stack are rebooted simultaneously.	If this situation happens, it is recommended that each power switch be rebooted in sequence with a four to five minute interval between each reboot.
Jumbo frames cause transmit errors on port channel	Transmit Errors is seen on port channel, but not on the members of the port channel. Counters remain inaccurate.	None – Inaccurate transmit errors do not cause functional issues.
PC8024F Stacking - CLI/WebUI : stack-ports counters value is always zero	CLI/WebUI shows the stack-ports counters value as zero after stack is formed.	None – Stack-Ports counter values as zero doesn't affect the PC8024F stacking functionality.
CLI command "no snmp-server community-group" doesn't work	CLI command "no snmp-server community-group" is not available.	None
Dot1x ias local authentication method not working	The internal database feature, which is a Dell specific feature, is not working correctly because this feature requires a user to authenticate using MD5, which is not supported by Windows at this time.	Use any other form of dot1x authentication.
"ipv6 pim join-prune interval" command is not working	CLI command ""ipv6 pim join-prune interval 30" does not change the default interval value from 60	None
Incorrect status being reported with show interfaces commands	When PowerConnect 8024F combo ports 21 and 22 are used for stacking, the show interfaces status command and show interfaces media-type commands report the status to be Detached and Down.	None
Power supply descriptions should be modified as "Internal" and "Remote" or "External" for main and secondary power supplies respectively in show system.	There is no impact to the user.	None
M8024-k Internal ports are up during most of the switch POST	Network operators may experience a single bounce during reboots of the M8024-k.	None
M8024, M6220, M8024k, PC8024F - Extra Lines and Tabs in CSR Cause CA Submittal Troubles	CSR may be rejected by Certificate Authority	Users can hand edit the CSR to left align all rows and eliminate blank lines before submission to the CA.
Sflow configurations do not get saved to the config	The operator entered a sflow command that takes a timeout value which makes the sflow configuration valid only for a fixed period of time. As the configuration is temporary (bound by the timeout value), it is not shown in running-config. Storing the vale in the running config/startup config would be an error as the time period may have already expired.	The configuration will show in the running config if the command is used with the "notimeout" option, e.g. *sflow 1 destination owner 1 notimeout*

Summary	User Impact	Workaround
Password strength - minimum characters not enforced	Operator may become confused regarding switch operations.	As is documented in the CLI Reference Manual, the password strength minimums do not become effective until the user has configured a non-zero value for *passwords strength minimum character-classes*. Please refer to the documentation for passwords strength minimum character-classes
M8024-k OpenManage Web UI stack view display	Operators using IE 8 may experience issues as follows: (1) Status LED does not glow to identify Master (2) Member units do not show "DELL PowerConnect M8024-k" model info (3) Member units port display is missing (4) LED label should be "Unit No." instead of "Stack No." ? (5) All Stack No. shown are as "01", instead of "01", "02", "03", "04" etc. (6) There are two "Slot 0" in display – confusing	Operators should consider using a browser other than IE 8.
Inline help for "spanning-tree loopguard" is incorrect.	The inline help indicates that the command applies to a single port.	Operators should be aware that this global CONFIG command applies to all ports.
show interfaces advanced firmware displays ports 1-20 as 10GBASE-T on 8024F	Operator should be aware that the type is reported incorrectly on this platform.	Ignore the type in the display for this command.
VLAN name config lost when upgrade from 3.1.5.16 to 4.2.x.x	When upgrading from release 3.1.4.16 to 4.2.0.4 the VLAN names only will not be copied to the upgraded configuration. VLAN numbers are not affected.	The user can cut the VLAN names and save these off before the upgrade occurs and then again reenter them after the upgrade.
Web GUI sFlow configuration , receiver owner inconsistent with CLI	Fails with an error - "Error! Failed to Set 'Receiver Owner' with " However, it is possible to save the same configuration (without receiver owner) via the CLI. Also, it is also not possible to add any polling device or sampler configuration on the Web GUI with this receiverIndex (seen in the show all option) since an error is thrown stating "Receiver Index is not configured".	Always configure the receiver owner when using the Web interface.
Websense: Order of switchport commands in running-config changed, Impacts scripts	The order that the commands “switchport mode general” and “switchport general allowed vlan” are displayed in the running config has been changed so that now the “allowed” command is first. This may cause problems with customer’s scripts that expect a certain order in the “show running-config” output.	None.
The “show dot1x statistics” command within the User Guide is actually “show dot1x interface statistics” command from the CLI.	The User Guide states that there is a “show dot1x statistics” command for displaying dot1x statistics on the switch when the actual command for doing this is “show dot1x interface statistics”. This can be frustrating to the customer if he has referenced the User Guide to look up the supposed correct command.	Use the “show dot1x interface statistics” command.

Release 4.1.1.9

Summary	User Impact	Workaround
LLPF is not supported on the PCM6220 switch	The hardware functionality needed to support LLPF is not available on the PCM6220 switch.	Upgrade to a PowerConnect switch that supports LLPF like a PCM6348 switch.
Traffic led solid green with 1Gb and 100Mb link speeds on PC8024/PC8024F	Setting advertisement from other switches or IXIA of 1Gb or 100Mb link speeds to 10G links on 8024, 8024F results in link up and traffic led to be solid green.	None – Traffic LED Solid Green do not cause any functional issues.
Config Lost for the Portchannel on removing a 2 Port 10 G Module on the PCM8024 switch	On boot up, the switch gives an error and rejects all the config for the portchannel as well as the TenGig interfaces in Bay1.	Remove port configuration of 10G module before removing the module from the bay and reboot the switch.

Release 4.1.0.19

Summary	User Impact	Workaround
Log message output	snmpwalk will report error log message related to CPU-port and vlan routing port	None – error messages do not cause functional issues.
Secure HTTP Random Characters	Under System Management -> Secure HTTP, random characters maybe populating some of the fields.	The CLI must be used to generate certifications.

Release 4.1.0.6

Summary	User Impact	Workaround
PC7XXX cable diagnostics for the Fiber ports does not work.	Fiber port cable diagnostics are not available for the PC7XXX.	None.
DUT delivers more power than the PD requested via LLDP in high power mode.	DUT may draw more power than negotiated at short cable lengths. PD may draw more power than negotiated, but power loss due to cable impedance is compensated for so that devices with average or longer cable length will receive adequate power.	None – system assumes 5.8W average loss due to cable length and delivers 5.8W extra power to ensure device receives requested power.
L3 routing NSF failover data plane on dynamic LAG - loss duration up to 5 seconds for large configurations	Interruption of voice, video and data service for duration of loss. Data plane loss during failover should not exceed 50 ms.	Disable portfast and auto-portfast on physical ports configured in a LAG.
Trunk mode VLANs transmit tagged frames only	Not compatible with other vendors trunk modes.	Administrators can configure “general” mode VLANs, which transmit PVID frames untagged and all other VLAN frames tagged. General mode is compatible with other vendor’s trunk mode behavior.
Speed/duplex commands available for interfaces which require auto-negotiation	Confusion about how to configure links.	Documentation and CLI prompt clearly states which commands are applicable to which interfaces. ***Only use speed/duplex commands on fiber interfaces. Only use speed auto/duplex auto commands on copper interfaces.***

Summary	User Impact	Workaround
ST : Stack member response times to ICMP ping requests in a 12 unit stack are larger than for stack master	No user impact expected. Observed occasional outlier response time up to 500 ms for stack members in a large stack configuration with heavy traffic. Average response time is well under 100 ms for stack members. All response times are well within ping limits.	None required.
Issue with protocol based VLAN configuration migration.	The command *vlan protocol group* required a string parameter in earlier versions; now it requires an integer parameter.	The software recognizes if the group name is alphanumeric, however it will not work when the name of the group is numeric (for example 2, 3, etc.).
Read/write user allowed read only access when authentication method is used as TACACS.	The user always gets Read-Only access if using TACACS as a means for HTTP authentication, even if the TACACS user is Read/Write capable.	User can configure the same TACACS user locally and use LOCAL authentication method for HTTP. The user will be able to get access based on the local user access level (Read-write or Read-only).
TFTP gives no reason for file download failures.	Generic failure message is issued.	Administrators can ping the TFTP server from the switch. Administrators should ensure the TFTP server is available, the requested file is available, and the permissions are set correctly.
CLI command stack-port config rejection does not display the cause.	If a user enters an invalid interface, a generic error message is issued.	Utilize the *show stack-port* command to identify stack port configuration issues.
The 'acct-port' command does not have 'no' version.	The user can configure the acct-port to the default using the positive form of the command	Configure the acct-port to the default using the *acct-port 1813* command in Radius accounting mode.
Non-configuration file getting loaded to startup-config through HTTP.	Switch does not utilize invalid configuration file information. Earlier versions of startup-config are not available for fallback when overwritten with an invalid startup-config.	In this case, an invalid configuration file was downloaded (on purpose) via the web. When the switch rebooted, it detected that the configuration file was invalid and overwrote the start-up config with the default configuration (an empty configuration). Users are advised to maintain off-line copies of switch configurations.
A v6 ping with the v4 header destination address set to 224.0.0.2 (all routers addr) is not responded to.	Users are not able to ping over 6to4 tunnels using IPv6 addresses.	Users can send pure IPv4 pings to the other end of the tunnel.
Certain packets match system rules that elevate the priority for protocol packets.	Packets may be transmitted out of order when using priority flow control. Additionally, if the queue that the packets are put on is not enabled for lossless PFC, then the packets can be transmitted even when the port was told to pause. This may have an effect on connections that expect packet order to be maintained, e.g. FCoE.	None.

Known Restrictions and Limitations

Release 5.1.0.1

Description	User Impact
SNMP walk is not successful while doing walk on root port	Low SNMP walk on root port may result in a timeout if executed without specifying any timeout value. Workaround: Execute walk with a recommended timeout value of 2 sec
The IPMC L2_BITMAP is only updated to reflect ports that should 'not' be flooded when a multicast stream is 'first' seen on a VLAN.	Moderate There will be some flooding of multicast traffic Workaround: Issue no ip multicast followed by ip multicast
"ip http secure-server" may not be cleared after performing the clear config operation if there is user intervention before prompt returns	Low Clear config operation clears all system components operational and configuration information and then builds the default configuration. This operation takes time to complete and the prompt may not be returned immediately. Prompt is returned after the completion of the operation. Please wait for the prompt, pressing "enter"/CR is not needed in this case. Workaround: Issue clear config one more time if “ip http secure-server” configuration is not cleared
Reboot needed when critical message “Failed to add local route for network X/X on interface X” appears on the console	High Route is not added and hence critical situation. Need a reboot to recover.

Release 5.0.1.3

System – 5.0.1.3

Stacking

Description	User Impact
Under certain conditions 5 or more ports identified as stacking ports can cause transmission errors even if the stacking links are not up.	Low This problem happens infrequently and setting those ports back to Ethernet mode has corrected the problem.

Release 5.0.0.4

System – 5.0.0.4

System

Description	User Impact
8100 switches increment “Internal MAC Rx Errors” counter, when packets are received with (size > 1518) and (size <= MTU size), and the packet contains an invalid FCS or code error detected or an IEEE length check error	Low For typical IP networks this problem won't be seen because the length field/Ethertype will contain a valid value.

Web

Description	User Impact
The device manager GUI does not support IE9 at this time.	Moderate – Multiple errors are displayed when trying to bring up the device GUI with IE9. Workaround: The User must use an Internet Explorer version prior to IE9 with the GUI. Note: This is not a limitation if running Release 5.1.0.1 or later versions of firmware.

iSCSI

Description	User Impact
“show iscsi sessions” command does not display established sessions on M8024/M8024-k/PC8024/PC8024F platforms.	Moderate – Workaround: Configure partner devices to send tagged, not priority tagged traffic.

Release 4.2.1.3

Management – 4.2.1.3

CLI

Description	User Impact
CLI command ‘show dot1x users’ is missing in CLI	Low – Use the show dot1x clients command to show the authenticated clients.
Show policy-map interface command does not take a port-channel parameter	Low – the administrator can show the counters on the individual members of the port-channel and sum them manually.
Show dot1x statistics command is missing in the CLI	Low – the administrator can show the statistics on the individual interfaces
Show crypto key pubkey-chain ssh - "username" option does not work	None – the administrator must configure and associate a key to a user in order for the user to be associated with an SSH key. The following example creates and associates an SSH user with a key: console(config)#username asd password XXXXXXXX privilege 15 console(config)#crypto key pubkey-chain ssh console(config-pubkey-chain)#user-key asd dsa console(config-pubkey-key)#key-string "ssh-dss AAAAB3NzaC1kc3MAAACBAJRwUAD3AuRACp1MObBeh1AgyZb18wf9Bt dip+t+1CbAqiqNEh4lBiew184DSKk0T6SnSSXuCN+bJnQPxJeiQt+OFnmjiYhn HcvI04Q5KnQhloZcEFgSsmQ7zJnReWtLvUQI0QvBIStanzedmQVGHvDrQ5X 2R729ToSH0ibBrnYtAAAAFQDNord7S9EJvUkKKxVBpWE6/skCmQAAAIB

	MjMO+BPP5KXzNWfZhqAhxBSoBvif/z6pzi9xWLlYy99A03zmRYCpcGIoLW iRHsR7NVpxFqwbqvez8KS0CDJ5aoKKLrpBlpg5ETkYEew/uTZ14lQQRBrzPw GBfxvTXKCWiI2j5KFa/WKLSnmWJX0/98qpxW/lMXoXsA9iK4pnMKwAAAI B4Jrt6jmoLybpzgOPOI0DsJ7jQwWacinD0jliz8k+qzCpanhd2wH+DEdj/xO2sFR fnYlME3hmXoB+7NByVUtheVjuQ2CWhcGFIKm9tbuPC6DtXh1xxT0NJ7rspv Lgb0s6y/0tk+94ZP5RCoAtLZ7wirShy3/KJ4RE0y2SFZjIVjQ==" console(config-pubkey-key)#exit console(config-pubkey-chain)#exit console(config)#exit console#show crypto key pubkey-chain ssh username asd Username : asd ssh-dss AAAAB3NzaC1kc3MAAACBAJRwUAD3AuRACp1MObBeh1AgyZb18wf9Bt dip+t+1CbAqiqNEh4lBiew184DSKk0T6SnSSXuCN+bJnQPxJeiQt+OFnmjiYhn HcvI04Q5KnQhloZcEFgSsmQ7zJnReWtLvUQI0QvBIStanzedmQVGHvDrQ5X 2R729ToSH0ibBrnYtAAAAFQDNord7S9EJvUkKKxVBpWE6/skCmQAAAIB MjMO+BPP5KXzNWfZhqAhxBSoBvif/z6pzi9xWLlYy99A03zmRYCpcGIoLW iRHsR7NVpxFqwbqvez8KS0CDJ5aoKKLrpBlpg5ETkYEew/uTZ14lQQRBrzPw GBfxvTXKCWiI2j5KFa/WKLSnmWJX0/98qpxW/lMXoXsA9iK4pnMKwAAAI B4Jrt6jmoLybpzgOPOI0DsJ7jQwWacinD0jliz8k+qzCpanhd2wH+DEdj/xO2sFR fnYlME3hmXoB+7NByVUtheVjuQ2CWhcGFIKm9tbuPC6DtXh1xxT0NJ7rspv Lgb0s6y/0tk+94ZP5RCoAtLZ7wirShy3/KJ4RE0y2SFZjIVjQ== Fingerprint : d9:d1:21:ad:26:41:ba:43:b1:dc:5c:6c:b9:57:07:6c SSH RSA or DSA keys can be generated by using the ssh-keygen command on a Unix system or with other publicly available utilities.
Broadcom NIC link always stays up within the m8024-k status even after disabling server port through device manager or turning off server altogether.	Low- This is works as designed and is necessary for new features for 12G. The Broadcom NIC 57810S never reports to the internal switch that the link is down because it needs the link to be up so that internal communications can continue with iDRAC and for other various components even after disabling the link on the server side.

Release 4.2.0.4

Layer 2 – 4.2.0.4

802.1x Authentication

Description	User Impact
Windows Vista® Authentication - The Windows Vista® client could fail to authenticate properly when the option to cache user credentials is selected.	Low Workaround: 1. In **Control Panel → Network Connections**, right-click on the desired **Local Area Connection** and select **Properties**. 2. In the **Properties** window, select the **Authentication** tab. 3. Deselect the checkbox for **Cache user information for subsequent connections to this network**. 4. Click **OK**.
The maximum number of 802.1x clients per port is 4.	Low – most deployments will have at most 2 802.1x clients per physical port. Note: If running Release 5.1.0.1 or later version of firmware, the maximum number is 24.
The maximum number of configurable traffic classes is 7.	Low as most deployments use a single traffic class. Some limited deployments may use up to 3 traffic classes.

MAC Filtering

Description	User Impact
Maximum number of unicast static filtering entries	The maximum number of unicast MAC and source port filtering entries is 20.
Maximum number of multicast static filtering entries	The maximum number of multicast MAC and source port filtering entries is 20. The maximum number of multicast MAC and destination port filtering entries is 256.
Static multicast MAC address table entries do not show with show command	Users must enable MAC filtering using the **mac addr-table multicast filtering** command to enable filtering. Static MAC multicast forwarding entries will then be shown.

LACP

Description	User Impact
LAGs Supported	Number of LAGs supported: 128 total LAGs of which up to 72 may be dynamic LAGs. Up to 144 ports can be assigned to dynamic LAGs. The PCM8024 supports 12 LAGs with up to 24 ports assigned to dynamic LAGs.

IGMP Snooping

Description	User Impact
No command to identify external IGMP querier	There is no specific command to identify an external IGMP querier. Administrators can use the **show ip igmp snooping querier detail** command or the s**how ip igmp snooping querier vlan** command to display information about snooping queriers.

Multicast VLAN Registration

Description	User Impact
MVR is not supported on LAGs	Use of MVR is restricted to physical interfaces.

Layer 3 – 4.2.0.4

IP MTU

Description	User Impact
IP VLAN MTU Support	Operators may see jumbo packets discarded when operating in a routed IP environment. ***Administrators are advised when operating in a L3 routing configuration with jumbo frames to adjust both the link MTU and the VLAN IP MTU.***

IPv6 MTU

Description	User Impact
IPv6 Fragmentation Support	The switch is not fragmenting the datagram and forwards even when the IP MTU of the forwarding interface is set to a lower value (than the datagram size). IPv6 frames are not allowed to be fragmented. IPv6 frames forwarded in silicon can be up to the lesser of 9216 octets or the link MTU. These frames are forwarded by the switching silicon with no effect. If a frame exceeds the link MTU for a port, it is discarded silently. If a packet is sent to the CPU or originated on the CPU and it exceeds the IPv6 MTU, then the packet still will not be fragmented. Instead, an ICMP error message is returned to the sender. The maximum IPv6 MTU is 1500 bytes. ***Administrators are advised that when operating in an L2 switching configuration with jumbo frames, to only adjust the link MTU and let the***

	system automatically adjust the IPv4/ IPv6 MTU based on the link MTU.

VRRP

Description	User Impact
The maximum number of VRRP instances is 50.	Users can scale VRRP higher than previously.

Management – 4.2.0.4

CLI

Description	User Impact
radius-server mode commands do not have a "no" form.	Low - None of the commands in radius-server mode support a "no" form except for the **msgauth** command. To reset values to the default, delete the server entry and add it back.
The maximum command line length is 1536 characters.	Low - Entries greater than the maximum line length throw an error, e.g. using multiple interface range qualifiers.

USB

Description	User Impact
Dir command can only address top-level directory on USB stick	Minimal – users can move files to top-level directory easily
Only FAT32 formatted devices are supported.	Minimal – FAT32 devices are the de-facto standard for flash devices
When multiple partitions are present on the flash drive, only the first partition is accessible.	Minimal – users will typically re-partition flash drives to maximize space.

Web

Description	User Impact
Certain browser (IE) versions respond slowly when displaying large lists of information. In these cases, the “All” display selection may not appear (is disabled).	This behavior is a browser performance limitation. Users may select another supported browser to enable “all” display functionality. Alternatively, the user may utilize the page selector functions to display the appropriate page of information.
Certain browser (FireFox) versions automatically block popups after a certain number of displays within a session.	This behavior is a browser functionality issue. If popups are blocked, the web interface will display errors/information using alerts. Users can disable popup monitoring by browsing to about:config and set dom.popup_maximum to -1

File Management

Description	User Impact
CLI Comment Character	The '!' indicates the beginning of a comment. All characters following the '!' will be treated as a comment (except when configuring a banner where the ! is accepted at the beginning of a line)

Data Center – 4.2.0.4

Interoperability

Description	User Impact
VLAN request/Notification counters are not incremented for priority tagged packets	Low – FIP sessions are established and are displayed in the show commands. FIP snooping VLAN request or VLAN response counters do not increment when CNA sends priority tagged frames (i.e. VID 0). It is observed that certain CNAs sometimes sends FIP VLAN discovery frames as 802.1Q tagged frames with VID=0 and priority as FCoE priority. FSB snoops FIP packets which are classified to any of FCoE enabled VLANs. In this case, the default VLAN (1) and the configured FCoE VLAN. In general, VLAN request messages are exchanged as untagged so gets associated with VLAN 1. In this case, the BROADCOM CNA sends priority tagged FIP frames (VID=0) which do not match the FSB snooping criteria because they do not get associated to any of the FCoE enabled VLANs hence FCoE VLAN Request/Notification counters are not incremented for priority tagged packets. These control frames are however are forwarded to FCF by FSB in order to establish a successful session. FIP snooping bridge need to consider forwarding priority tagged FIP frames to FCF as well in order to interoperate with CNAs which could send priority tagged packets. The current FSB implementation does this already.
Broadcom CNA only supports configuration of VLAN via VLAN Discovery process	Low – Most users prefer automatic setup of CNAs The Broadcom CNA does not support manual configuration of VLAN. This means that customers who prefer to set up their FCoE network manually will not be able to do so if using BRCM CNAs.
FIP snooping bridge does not forward the DCBX FIP tlv info from configuration source	Low – No supported FCF supports this configuration option. While working with QLogic, it is found that CNA sends two TLVs concerning the FIP/FCoE traffic. It sends FIP TLV along with FCoE TLV with respective priorities - in this case same priority for both. Although, it is not a normal use case but can be used to have different treatment for control and data traffic. There can be a use case where host or FCF can choose to create different priorities for control (FIP) and FCoE data traffic. In cases, where FIP and FCoE use different priorities, it is expected that intermediate switches are configured to treat them accordingly. In cases where ports are configured in DCBX auto mode and configuration source carries two TLVs, one for FIP and other for FCoE with different priorities then it is expected that FSB/DCB should forward this information to downstream ports. The PowerConnect FSB implementation ignores the FIP TLV and does not forward this information to the peers. In such cases, Host will not know the special treatment or expected priority for FIP frames. Considering that slow protocol and this being a corner case situation, this can be a readme and documented in release notes.
FIP Snooping Over Stack Results in eNode in Ethernet VLAN	Low - When trying to accomplish FIP snooping over the stack, the eNode address is put in the wrong VLAN causing the connections to never occur. FCoE is not supported across the stacks so this is a non-issue.

End of Release Notes