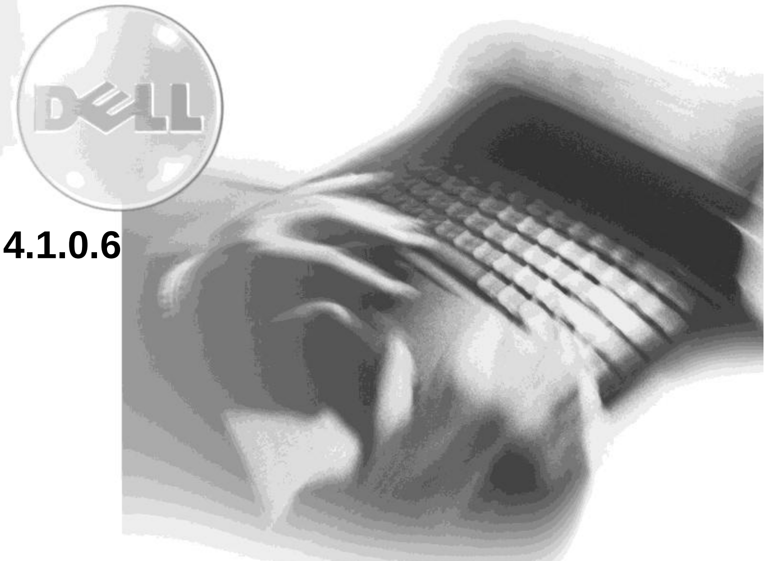
Dell™ PowerConnect™
7024/7048/7024P/7048P/7024F/7048R/7048R-RA/8024/8024F/
M6220/M6348/M8024/M8024-k

PowerConnect
4.1.0.6 Firmware Release Notes



Date: March 2011
System Firmware Version 4.1.0.6

Information in this document is subject to change without notice.

Table of Contents

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

Introduction

This document provides specific information for the Dell PowerConnect 7024/7048/7024P/7048P/7024F/7048R/7048R-RA/8024/8024F/M6220/M6348/M8024/M8024-k switches firmware version 4.1.0.6.

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 No.	Release Date
PCM6220v4.1.0.6.stk	**4.1.0.6**	**March 2011**
PC7000_M6348v4.1.0.6.stk	**4.1.0.6**	**March 2011**
PC8024v4.1.0.6.stk	**4.1.0.6**	**March 2011**
PCM8024v4.1.0.6.stk	**4.1.0.6**	**March 2011**
PCM8024kv4.1.0.6.stk	**4.1.0.6**	**March 2011**

Version Numbering Convention					
Version number					**Description**
PowerConnect Series	4	1	0	6	Four part version number
				↑	Denotes the build number.
			↑		Denotes an ad hoc release of the product software.
		↑			Denotes a scheduled maintenance release of the product software.
	↑				Denotes a major version number.

Firmware Version Details

Boot PROM Name	Version No.	Release Date
Not Applicable	4.1.0.6	March 2011

Firmware Upgrade

NOTE: Switches migrating from pre-4.x.x.x versions of code require a boot code update. Connect to the serial port and follow the procedure below to update the boot code:

1. Download the new firmware version to the switch
2. After the download completes, activate the new image using the *boot system image* command
3. Reload the switch using the reload command
4. After the switch boots, select *2 – Start Boot Menu*
5. Select *7 – Update Boot Code* from the menu
6. After the boot code updates, select *9 – Reset the system*.

NOTE: By default, switches in a stack configuration will upgrade or downgrade stack members with the firmware version installed on the master switch.

Supported Firmware Functionality

For more details regarding the functionality listed below, please refer to the Dell PowerConnect Series CLI Reference Guide and the Dell PowerConnect Series Configuration Guide.

Firmware Downgrade

Downgrading from 4.1.0.6 to a previous release is supported on the PowerConnect series switches. It is not recommended to downgrade the boot code under any circumstances.

Hardware Supported

- 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	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	✓		✓				

Added Functionality in this Release

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

- ➢ 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 regarding system events. Multiple email addresses can be configured. The system will attempt to resolve mail servers specified with a DNS 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 new authentication servers. Users attempting to authenticate using the authentication server 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 cause the time range to not be 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 switch administrator 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 configuration 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. Only the RADIUS and TACACS methods can fail and therefore should be specified first in an authentication list. The other methods will never fail and therefore should be specified after RADIUS or TACACS in a list.

The 802.1x authentication list cannot be named and only supports the RADIUS, IAS, or none authentication methods. 802.1x authentication supports a single authentication method, not a list of methods.

- 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 users are not given management access to the switch. IAS users, once authenticated, can only pass frames across the switch.

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 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 File. 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 file.

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 sufficient number of *exit* commands are present in user defined macros to return the prompt to the level at which it was entered when the macro is invoked.

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 PCM6348/PCM6220/PCM8024/PC8024/PC8024F 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 PCM6348/PCM6220/PCM8024/PC8024/PC8024F switches may lead to unexpected results.

- New Web Interface

  The Web interface has been enhanced with new navigation feature 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.

- 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. Rear panel slots are number 1 and 2. Front panel ports belong to slot 0.

  The service port is 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.

- All Interfaces Default to VLAN 1

  By default, all in-band interfaces are members of VLAN 1. The operator may exclude ports from VLAN 1 via configuration.

- Routing Supported on VLANs Only

  Routing is only supported on VLAN interfaces. Routing may not be configured on a physical interface.

- Assigning IP Address Enables Routing

  Assigning an IP address to a VLAN enables routing on the 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 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, all VLANs are members of a trunk port. VLANs created after a trunk port is created are added to all trunk ports. VLANs deleted by the administrator 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 enabled 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 is a VLAN member. 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,…) 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 in this release. The issues listed here may have been discovered on any of the switches listed on the title page.

Summary	User Impact	Workaround
SSH crash - memPartAlloc: block too big	Reduced switch functionality.	Memory allocation issue is corrected and checked for memory leaks
PC M8024 switch reset out-of-band address to none when switchports were changed	Inability to access switch via OOB port.	The out-of-band address is maintained over switchport changes.
Web page shows IP address as '0.0.0.0' for '1.1.1.1' routing interface.	Operator confusion over switch operations	The web page output has been corrected.
Read-Only Web page is populating all configured IP and IPv6 ACL names when we select the ACL Name.	Operator confusion regarding web page operations.	The web page has been corrected to only populate the selected entry.
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
Incorrect command is being displayed in running-config, when disabled the boot host dhcp	Operator confusion regarding web page operations.	The running config now shows the correct configuration
DUT crashes while configuring max dynamic vlans.	Network outage possible.	The PowerConnect does not crash when using maximum dynamic VLANs
Manager of the stack is changing when trying to learn maximum number of VLANs using GVRP.	Operator confusion regarding switch operations.	The stack manager does not change during learning with GVRP
Switch prompts to save config data when no changes have been made	Operator confusion regarding switch operation.	The switch no longer prompts to save config data if no changes have been made
Crash while RFC3918 Group Capacity test is running	Network outage possible.	The PowerConnect switch runs the RFC3918 test without crashing
'no' version of 'key' command is not implemented	Operator frustration with switch management.	The **no key** command is implemented to return the key configuration to the default.
Password is not accepting quotation (") character	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.
Incorrect warning message displayed while executing the command "boot system <unit> image1"	Operator confusion regarding switch operation.	The error message has been corrected to indicate that the unit selected for reboot does not exist.
IPV6 command displays wrong output	Operator confusion regarding switch operation.	The IPv6 output has been corrected to remove the duplicate display lines in **show ipv6 help.**
LLDP-MED log messages showing 5 sec difference in entry age out information	Operator confusion regarding switch operation.	The LLDP timer has been updated to account for processing skew.
Dhcpv6 web issues	Operator confusion regarding switch configuration.	The acceptable character sets are documented in the CLI Reference guide.
LLDP MED application should not allow configuration of location and inventory transmit TLV's as underlying application not present	Operator confusion regarding switch configuration.	Location and inventory TLVs cannot be enabled for transmission in LLDP MED.

Summary	User Impact	Workaround
SysUpTime is not being shown correctly during an SNMP walk (Poll interval 1sec)	Operator confusion regarding switch operation.	The correct variable is used to write SysUpTime
Log messages need to be corrected on ip dhcp snooping rate limit scenario.	Operator confusion regarding switch configuration. Inability to diagnose network issues.	Interface representations in log messages use unit-slot-port format.
The **show ip vlan** command output is not proper after more-quit prompt is encountered, i.e. after around 16 routing interfaces	Operator confusion regarding switch configuration.	The paging has been corrected.
Invalid error port number displayed on log message when vlan is changed to forbidden mode from access mode	Operator confusion regarding switch configuration.	The error message is no longer issued.
The **banner motd XXXXX** does not appear in show running-config	Operator confusion regarding switch configuration.	All banner configuration appear in the running-config
Web page mac-vlan table too slow to load.	Operator frustration with switch management.	For certain browsers, paging has been implemented to speed up load times.
Confused between **ip default gateway** and **ip default route** (update manual with how to set a default route).	Operator confusion regarding switch configuration.	The ip default route command is deprecated. Use the **ip default route** command to set a default route.
Auto Install **show boot retry** count line needs to be left aligned by one space.	None.	The retry count alignment is corrected
Cannot Access Optical Transceiver Diagnostics Page if Multiple Submits done prior to initial refresh completing	Operator frustration with switch management.	This is a browser dependant issue (IE 6) that is not seen in later versions. The web session recovers after doing a refresh.
Error messages for non-existent stack members non-informative	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.
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 **no ipv6 forwarding** command.
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.
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
Block command is not seen in show running config through web and cli	User confusion over switch operations.	The block command is a temporary administrative assignment and is not maintained persistently in the saved or running configs.
FDB entries are getting aged out before default age-out time, when both FDB and MFDB tables are full.	User 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.
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.
Configuring all ports in all VLANs takes a long time	Operator frustration with switch management.	VLAN configuration has been optimized.

Summary	User Impact	Workaround
Max number of OSPF neighbors not supported	User confusion over switch operations.	The maximum number of neighbors is supported.
Cable fault distance not getting displayed in WEB in case of cable with one or more pairs cut or short.	User confusion over switch operations.	The fault distance is displayed in the web page.
Ports representation need to be changed in debug messages	User confusion over switch operations. Inability to diagnose network issues.	Ports are now displayed in C/S/P standard format
No error message for illegal characters in various command parameters	User confusion over switch configuration.	The accepted character set and length is documented in the CLI reference manual.
The ARP entry is not seen in the ARP table when an ARP reply is sent to DUT.	User confusion over switch operations. Inability to diagnose network issues.	ARP entries are stored properly
Mapping Table configuration is not being displayed on Read-Only mode user web page.	User confusion over switch configuration.	The mapping table is displayed for a read-only user.
ACL is getting deleted when trying to create max+1 rule.	User confusion over switch operations. Possible security issues.	Corrected error checking logic.
LLDP-Med TLV information not registered for jumbo frame sizes greater than 8000	User confusion over switch operations.	Jumbo LLDP frames are now processed properly
VLAN binding entries are not being displayed on Read-Only mode user web page.	User confusion over switch operations.	VLAN binding entries are available to read only users
Unable to execute the command dot1x timeout tx-period 1	User confusion over switch operations.	This command is accepted with a timeout period of 1 second. Corrected range check on input.
In switching> network security >dot1x authentication web page in read-only user mode, the Re-Authenticate Now check box can be checked	User confusion over switch operations. Possible security issue.	Read-only properties are set for the check box
System Device information web page LED information not in sync with front panel LED information.	No user 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
DHCP snooping static binding thru DHCP request is denied as this is a expected behavior.	User 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.
Mode of transfer is displaying “unknown,” while downloading the code from ftp	User confusion over switch operations.	ftp transfer mode is displayed
Allow disabling and enabling of terminal paging	User frustration over switch configuration.	The terminal length command is now implemented.
Web does not allow to configure image descriptor to its max length i.e. 255 characters.	User confusion over switch operations.	Images descriptors up to 255 characters are allowed

Summary	User Impact	Workaround
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.	User 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.
CLI Manual Has No Index	User frustration over switch configuration.	The CLI manual has an index
Script validation is fails when max SNTP servers are configured.	User confusion over switch configuration.	Corrected CLI validation check so that existing server can be entered multiple times.
Configured SYSLOG server parameters cannot be updated without deleting and re-configuring	User frustration over switch configuration.	Syslog server parameter can be updated in the CLI without deleting the server
CLI will not let user configure available parameter for the given IGMP command	User frustration over switch configuration.	IGMP configuration commands can be entered in interface VLAN mode at any time
Inconsistent behavior - using same port number for multiple services	User 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.
LLDP Assignment of port ID for Port-Description TLV	User 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
Management ACL list needs "Match every packet" option	User 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.
SNMP support for Dell-LAN-TRAP-MIB	User frustration over switch configuration.	The Dell-LAN-TRAP-MIB is supported

CLI Reference Guide Updates

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

None required.

Known Issues

Summary	User Impact	Workaround
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.***
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.

Summary	User Impact	Workaround
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

Layer 2

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. 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**.
Maximum number of 802.1x clients per port	The maximum number of 802.1x clients per port is 4.
Maximum number of 802.1p traffic classes	The maximum number of configurable traffic classes is 7.

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: • 48 total LAGs of which up to 18 may be 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

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 to only adjust the link MTU and let the system automatically adjust the IPv6 MTU based on the link MTU.***

IP Routing

Description	User Impact
Static IP routes do not show with the **show ip route** command	The switch UI will attempt to discourage the configuration of static ip route entries for which a matching subnet does not exist. Certain configuration sequences may still allow such routes to be configured. Configuring an IP address on a VLAN which matches the next hop IP address of the static route in all significant bits will allow the display of the route using the show command.
VRRP VRID limit is 20.	The switch will only support VRRP environments with 20 or less VRRP routers.

Management

CLI

Description	User Impact
radius-server mode commands do not have a "no" form.	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.

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.
Certain devices, e.g. Kingston DataTraveler may report erroneous information for items such as free space.	Minimal – these flash devices are still usable. User may erroneously copy a large file onto the drive when insufficient space is available.

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.

End of Release Notes