Dell™ PowerConnect™ 6224/6224F/6224P/6248/6248P

PowerConnect 6224/6224F/6224P/6248/6248P Release Notes

Date: May 2010
System Firmware Version 3.2.0.6

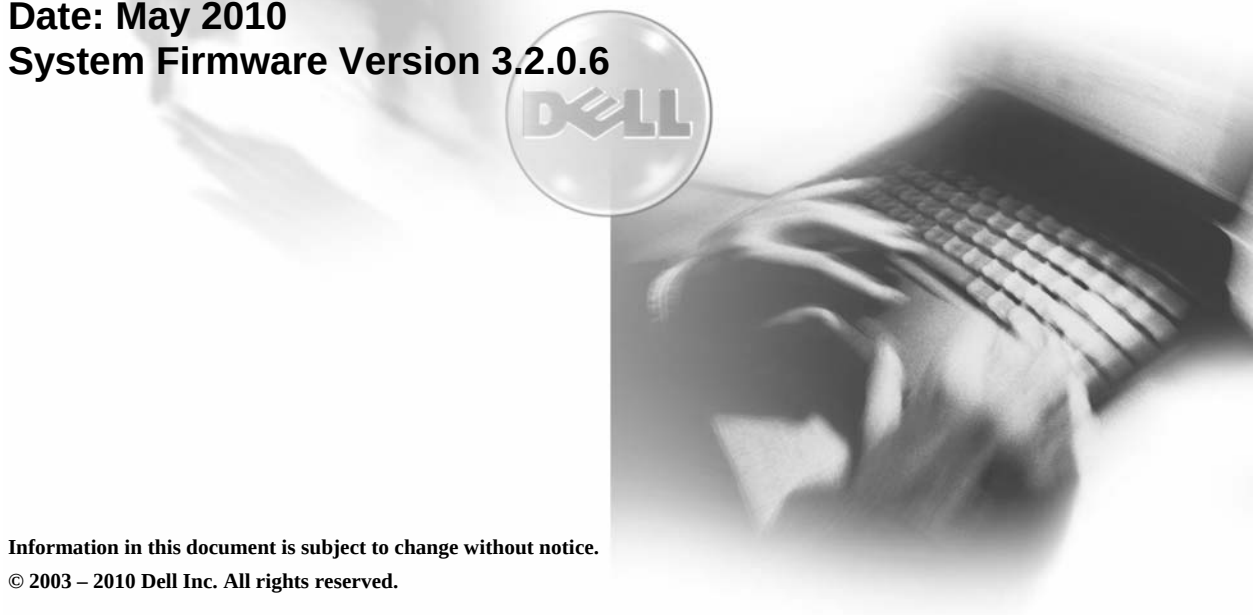

Table of Contents

PowerConnect 6224/6224F/6224P/6248/6248P Release Notes

Introduction

This document provides specific information for the Dell PowerConnect 6200 Series switches, firmware version 3.2.0.6.

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 the Support Web Site http://support.dell.com/.

Firmware Specifications

Firmware Version Details

Boot PROM Name	Version No.	Release Date
Not Applicable	3.2.0.6	May 2010

Firmware Upgrade

NOTE: Version 3.2 includes improvements to the firmware management system. You MUST follow the procedure set forth in the Dell PowerConnect 6200 Series Release 3.2 Upgrade Procedure included in the zip file to update the boot code AND firmware. Failure to adhere to this procedure may result in your switch becoming inoperable.

NOTE: The PC6200 switches when stacked require that the same version of firmware be installed on every switch member.

Firmware Image Name	Version No.	Release Date
PC6200v3.2.0.6.stk	3.2.0.6	May 2010

Version Numbering Convention					
Version number					**Description**
6200 Series	3	2	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.

Supported Firmware Functionality

For more details regarding the functionalities listed, please refer to the Dell™ PowerConnect™ 6200 Series Systems CLI Reference Guide and the Dell™ PowerConnect™ 6200 Series Configuration Guide.

NOTE: OMNM 4.1 will not discover the switches running any version of 3.x.y.z firmware therefore users should upgrade to version 4.2.

If you use OpenManage Network Manager to deploy firmware, do not use it to deploy 3.x (or later) firmware to a PowerConnect 62xx device that is currently running firmware version 2.x or earlier. Only use the method described in these Release Notes to upgrade this firmware.

Firmware Downgrade

Downgrading from 3.2.0.6 to a previous release is not supported. Users should save their configuration file to a backup location before performing this operation.

Hardware Supported

PowerConnect 6224

PowerConnect 6248

PowerConnect 6224F

PowerConnect 6224P

PowerConnect 6248P

Added Functionality in this Release

- Non-Stop Forwarding

  This feature creates an option to allow the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the stack management unit. This type of operation is called non-stop forwarding. When the management unit fails, only the management switch needs to be restarted.

- Configuration of CX-4/Stacking Modules

  This feature will allow the stacking and CX-4 plug-in modules to be configured to either role (Ethernet or Stacking). By default, the module will function according to its module ID. Upon changing the role of a module, a reboot of the switch will be required for the change to take effect.

- Custom Protocol Based VLANs

  Prior to the 3.2 release only ARP, IP and IPX are configurable as protocols for protocol-based VLANs. This has been extended so that any Ethertype may be used.

- Port Configuration Show Command

  Added support for a single command that shows VLAN, STP, Port Status, and Port Configuration information etc.

  The new command is **show interfaces detail {ethernet** interface | **port-channel** port-channel-number} where
  - interface—A valid Ethernet port.
  - port-channel-number—A valid port-channel trunk index.

- Configurable Message of the Day Banner

  The system supports a configurable message of the day banner that displays on the console. This feature is configurable via the CLI or GUI and supports 1500 characters.

- VLAN Name Support with RADIUS Server

  This feature is an extension of Dot1x Option 81 feature added in Power Connect Release 2.1 to accept a VLAN name as an alternative to a number when RADIUS indicates the Tunnel-Private-Group-ID for a supplicant. Since this option is a string, it can also be used for a VLAN name. In order to support this feature, VLAN names must be unique.

- HTTP Download

  Allow users to download files via an HTTP session. All file types which may be downloaded via TFTP are supported.

- Serviceability Tracing Commands

  Debug commands provided to enable tracing of various protocols.

- Faster Initialization for Stacking Failover

  Fast Reinitialization involves improvement in:

  - Detection of Management Unit Failure
  - Building Card Manager Database
  - Application of saved configuration

  Performance Improvements (based on Configuration File size) are:

  - Default ~ 35%
  - Medium ~ 50%
  - Large ~80%

  The impact is higher on large configuration files versus the smaller ones.

- Auto Config

  Auto Config is a software feature which provides for the configuration of a switch automatically when the device is initialized and no configuration file is found on the switch. Auto Config is accomplished in three phases:

  1. Configuration or assignment of an IP address for the device
  2. Assignment of a TFTP server
  3. Obtaining a configuration file for the device from the TFTP server

- DHCP Snooping

  DHCP Snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server. It filters harmful DHCP messages and builds a bindings database of (MAC address, IP address, VLAN ID, port) tuples that are specified as authorized. DHCP snooping can be enabled globally and on specific VLANs. Ports within the VLAN can be configured to be trusted or untrusted. DHCP servers must be reached through trusted ports.

- DHCP L2 Relay

  Permits L3 Relay agent functionality in L2 switched networks.

- sFlow

  sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

- MLD Snooping (RFC2710)

  In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address.

  In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports intended to receive the data (instead of being flooded to all of the ports in a VLAN). This list is constructed by snooping IPv6 multicast control packets.

- MGMD Proxy

  The IGMP Proxy component has been extended to include support for MLD Proxy and is now called the Multicast Group Membership Discovery (MGMD) Proxy. The MGMD Proxy is used to enable the system to issue MGMD host messages on behalf of hosts that the system discovered through standard MGMD router interfaces, thus acting as proxy to all its hosts residing on its router interfaces.

- Dynamic ARP Inspection

  Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

- Multiple LLDP Neighbors per Interface

  This feature allows support for multiple neighbors on a single LLDP interface.

- Configurable DSCP for Voice VLAN

  Allow the user to configure the voice VLAN DSCP parameter and set the DSCP value. This value is retrieved by LLDP when the LLDPDU is transmitted (if LLDP has been enabled on the port and the required TLV is configured for the port).

- CDP Interoperability

  Allows the ISDP feature to interoperate with Cisco™ devices running CDP.

  Industry Standard Discovery Protocol (ISDP) is a proprietary Layer 2 network protocol which inter-operates with Cisco network equipment and is used to share information between neighboring devices (routers, bridges, access servers, and switches).

  This feature is enabled by default if using phones with CDP enabled, but should be disabled if a Voice VLAN is manually configured on the port.

- SSH/SSL Refresh

  The SSH update incorporates the latest security and bug fixes.

- RADIUS Enhancements

  - The maximum number of RADIUS servers supported has increased from three to 32.
  - RADIUS servers with the same name can be used as Backups (RADIUS Authentication and Accounting servers)
  - Simultaneous Transactions to Multiple RADIUS Servers
  - RADIUS Accounting – Allows a client the ability to deliver accounting information about a user to an Accounting server.

- IPv6 support for QoS (ACL/DiffServ)

  Extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification. Ethernet IPv6 packets are distinguished from IPv4 packets by a unique Ethertype value (all IPv6 classifiers include the Ethertype field).

- Auto VoIP

  This provides ease of use in configuring VoIP for IP phones on the switch. This is accomplished by enabling a VoIP profile that a user can select on a per port basis.

- Dynamic ACL Management

  The number of rules allowed per ACL has been increased to the maximum allowed by the silicon (127 rules). This will allow all available rules to be assigned to a single ACL. However, the user is no longer guaranteed to be able to apply an ACL if the number of rules is over-subscribed. Refer to the Configuration Guide for details.

- SCPv2, SFTP

  Adds the ability for the user to securely transfer files to/or from the switch. It makes use of the Secure Copy Protocol (SCP) and SSH File Transfer Protocol (SFTP). SSH client login is used to establish a secure connection to the remote server before the file transfer begins.

- Captive Portal

  This allows administrators to block clients from accessing the network until user verification has been established or authenticated. Verification can be configured to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted.

- 802.1x MAC Authentication Bypass (MAB)

  Provides 802.1x unaware clients controlled access to the network using the device MAC address as an identifier. This requires that the known and allowable MAC address and corresponding access rights be pre-populated in the authentication server. MAB only works when the port control mode of the port is MAC-based.

- Ping/Traceroute Enhancements

  New ping options have been added to allow the user to specify the number and size of echo requests and the interval between echo requests. A ping can now be initiated via SNMP using the MIB defined in RFC 2925.

  New traceroute options have been added to allow the user to specify the initial and maximum time to live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe. A trace route can be initiated in the web and SNMP user interfaces.

- Static Reject Routes

  Allows the user to configure a static route to discard the packets to a particular destination, thereby forcing a black-hole routing behavior for a particular set of IP prefixes.

  This can be done for the following reasons:

  - Prevent a routing loop in the network (default route configured on a router).
  - A preventive measure against a DOS attack on a router with unwanted destination addresses.

- Clear ARP Cache Management Port

  A new CLI command has been added to enable clearing of the ARP table of entries learned from the management port.

- OSPFv2 Point-to-Point Links

  OSPF can treat an interface as a point-to-point circuit, even though the physical network is a broadcast network. This simplifies OSPF operation on the link. OSPF does not elect a designated router for a point-to-point network, and does not generate a network LSA to represent a point-to-point network in the link state topology. This mode of operation is useful when there are only two routers attached to the link (either a physical or virtual LAN).

  In point-to-point mode, OSPF joins the AllSPFRouters multicast group on the interface and sends all OSPF packets on the interface to AllSPFRouters. OSPF accepts packets received on point-to-point interfaces even if the source IP address is not on a local subnet.

- OSPVv2/v3 Summary Reject Routes

  The area address range advertised by OSPF router at area boundaries as summary route into another area can lead to routing loops in some situations. This feature can avoid situations where a routing loop can occur in a network.

- OSPF v2/v3 Passive Interfaces

  Allows passive interfaces for OSPF implementations.

- Granular OSPF v2/v3 Traps

  Configure which of the OSPF traps the OSPF Router should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the OSPF router will send the trap to all trap receivers.

- **auto-cost reference bandwidth** and **bandwidth** Commands

  Controls how OSPF calculates the default metric for an interface by using the auto-cost command in router OSPF configuration mode. To assign cost-based only on the interface type, use the no form of this command.

- **network area** Command

  Support is added for the following 2 OSPFv2 CLI commands:

  - **network** *ip-address wildcard-mask* **area** *areaid*
  - **ip ospf area** *areaid* **[secondaries none]**

- OSPF v2/v3 Route Preferences Rework

  The following effects are seen with this change:

  - Configuration of external route preference that applies to all OSPF external routes (like type1, type2, nssa-type1, nssa-type2) equally.
  - Allows multiple route types to be configured with equal preference values.
  - No longer follows the order among OSPF route preferences: intra < inter < external.
  - Configuring the route preference of 255 makes the route ineligible to be selected as the best route to its destination (a route with preference of 255 is never used for forwarding).
  - While migrating from previous releases, the preference for the external routes will be set with the preference value of the type-1 route in the earlier releases.

- Opaque LSAs and Detailed Display of OSPF v2 LSAs

  Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by some application wishing to distribute information throughout the OSPF domain. For example, the OSPF LSA may be used by routers to distribute IP to link-layer address resolution information.

- ICMP Enhancements (RFC4443)

  ICMPv6 code is updated to support RFC 4443.

- DNSv6 Client

  The DNS Client has added support for IPv6 (RFC3596). The transport for communication with a DNS server can be either IPv6 or IPv4 depending on type of server address.

- Configured Tunnels MTU

  To comply with RFC 4213, Basic Transition Mechanisms for IPv6 Hosts and Routers, the IPv6 MTU on configured IPv6 over IPv4 tunnels was changed from 1480 bytes to 1280 bytes.

- IPv6 6 to 4 Auto Tunnels

  The 6 to 4 tunnels automatically formed IPv4 6 to 4 tunnels for carrying IPv6 traffic. The automatic tunnel IPv4 destination address is derived from the 6 to 4 IPv6 address of the tunnel next hop. There is support for a 6 to 4 border router that connects a 6 to 4 site to a 6 to 4 domain. It sends/receives tunneled traffic from routers in a 6 to 4 domain that includes other 6 to 4 border routers and 6 to 4 relay routers.

- VRRP Route Interface Tracking

  This extends the capability of the Virtual Router Redundancy Protocol (VRRP) to allow tracking of specific route/interface IP state within the router that can alter the priority level of a virtual router for a VRRP group.

  The exception to this is, if that VRRP group is the IP address owner, its priority is fixed at 255 and can not be reduced through tracking process.

- ICMP Throttling

  This adds configuration options for the transmission of various types of ICMP messages.

  This project adds the following configuration options:

  - Rate limiting the generation of ICMP error messages.
  - Suppression of ICMP echo replies.
  - Suppression of ICMP Redirects.
  - Suppression of Destination Unreachables.

- IP Helper

  Provides the ability to enable DHCP relay on specific interfaces, with DHCP server addresses specified independently on each interface. The **ip helper-address** commands configure both DHCP and UDP relay.

- OSPF Enhancements

  A CLI command is added with options to do the following:

  - Disable and re-enable OSPF
  - Clear the OSPF configuration
  - Bounce all or specific OSPF neighbors
  - Flush and re-originate all self-originated external LSAs
  - Clear OSPF statistics

- Support of IPv6 routes in PIM-SM and PIM-DM

  Support for IPv6 routes has been added to PIM-SM and PIM-DM.

- IPv6 Management Enhancements

  Provides the following:

  - Dual IPv4/IPv6 operation over the network port
  - Static assignment of IPv6 addresses and gateways for the service/network ports
  - Ability to ping an IPv6 link-local address over the service/network port
  - SNMP traps and queries via the service/network port

- Updated IPv4 Multicast Routing Support

  The Multicast package code has been extensively re-engineered and furnished with the following:

  - PIM-DM advanced to RFC 3973
  - PIM-SM advanced to RFC 4601, pim-sm-bsr-05, draft-ietf-pim-mib-v2-03
  - DVMRP advanced to draft-ietf-idmr-dvmrp-v3-10.txt, draft-ietf-idmr-dvmrp-mib-11.txt

- MLD Snooping Querier

  MLD Snooping Querier is an extension to the MLD Snooping feature; it enhances the switch capability to simulate a MLD router in a Layer 2 network thus removing the need to have a MLD Router in a Layer2 network to collect the Multicast group membership information. The Querier functionality is a small subset of the MLD Router functionality.

Changed Functionality in this Release

- Spanning Tree Update – 802.1Q-2005

  Spanning Tree now supports IEEE802.1Q-2005. This version of the IEEE Multiple Spanning Tree Protocol corrects problems associated with the previous version, provides for faster transition-to-forwarding, and incorporates new features for a port (restricted role and restricted TCN).

  Restricted role - Setting the restricted role parameter for a port causes the DUT not to select that port as a root for CIST or any MSTI.

  Restricted TCN - Setting the restricted TCN parameter causes the port not to propagate topology change notification. A port configured with this parameter will not flush its MAC address table or send out a BPDU with a topology change flag set to true when it receives a BPDU with the topology change flag set to true.

  Hello-time - This revision of the standard does not allow the value of hello-time to be modified; consequently, the hello-time command has been blocked for all CLI.

  Loop Guard - The STP Loop Guard feature is an enhancement of the Multiple Spanning Tree Protocol. STP Loop Guard protects a network from forwarding loops induced by BPDU packet loss. It prevents a blocked port from erroneously transitioning to the forwarding state when the port stops receiving BPDUs.

  The reasons for packet loss are numerous, including heavy traffic, software problems, incorrect configuration, and unidirectional link failure. When a non-designated port no longer receives BPDUs, MSTP considers this link as loop free and begins transitioning the link from blocking to forwarding. In forwarding state, the link may create a loop in the network.

  Enabling loop guard prevents such accidental loops. When a port is no longer receiving BPDUs and the max age timer expires, the port is moved to a “loop-inconsistent blocking state.” In the loop-inconsistent blocking state, traffic is not forwarded (acting in the same manner as the blocking state). The port remains in this state until it receives a BPDU and it transitions through the normal spanning tree states based on the information in the received BPDU. Normal spanning tree states include blocking, listening, learning, and forwarding.

  The “loop-inconsistent blocking state” is a state introduced with the loop guard feature.

  This feature is intended for improving network stability and used for preventing STP loops. It is compatible with CST, RSTP and MST modifications of spanning tree.

  Note: Loop Guard should be configured only on non-designated ports. These include ports in alternate or backup roles. Ports in designated roles should not have loop guard enabled. Ports in designated roles can forward traffic.

- RFC3621 (PoE) MIB Moved

  The POWER-ETHERNET-MIB has been moved from its previous location of {fastpath 16} to the standard location of {mib-2 105}. Any SNMP agents that accessed this MIB on previous releases must be updated to use the new location.

- RFC1612 (DNS Resolver) MIB Moved

  The DNS-RESOLVER-MIB has been moved from its previous location of {fastpath 200} to the standard location of {dns 2}. Any SNMP agents that accessed this MIB on previous releases must be updated to use the new location.

- **ip route** Command Changed

  The syntax of the **ip route** command has changed. The metric keyword is no longer accepted as it had no effect. The new syntax is:

  ip route *ip addr subnetmask* | *prefix-length nextHopRtr* [*preference*]

- **distance ospf** Command Changed

  The **distance ospf** command has been changed (for both OSPFv2 and OSPFv3) to the industry standard syntax. The new syntax is:

  distance ospf {**external** | **inter-area** | **intra-area** } *distance*

- **ip mtu Command** Changed (Maximum Value Increased)

  The maximum value for the **ip mtu** command has increased from 1500 to 9202. If not configured, the IP MTU tracks the interface MTU.

- **bridge address** Command Changed

  The following **bridge address** command optional parameters have been deprecated:

  - **delete-on-reset**
  - **delete-on-timeout**
  - **secure**

- **port security** Command Changed

  The following port security command optional parameters have been deprecated:

  - **forward**
  - **discard-shutdown**

- Link Dependency Available

  The Link Dependency feature which has previously only been available on modular switches is now available on all switches. The functionality is similar to the capability available on the PCM6220, PCM8024, and the PCM6348.

  This release added an action capability to link-dependency where if a dependant port goes down, as an action option, the group's members come up versus also go down. This can be used as a form of link redundancy as an alternative to using STP.

- ISDP Advertise/Display hostname

  ISDP can now use the hostname as the Device ID instead of the Serial Number. The user needs to change the default hostname on the switch and can verify the results via the **show isdp** command.

- Trap Configuration

  In previous versions of the software, configuration of the flags for controlling traps was scattered about in a number of places.

  snmp-server enable traps is now a common command for configuring all trap flags. The legacy commands are preserved for backward compatibility. Also note that the keyword “trap” has changed to the plural “traps”.

- SNTP Server Priority

  The server priority is now available from the **show sntp configuration** command. Previously it was only configurable.

- GARP Leave Timer

  The valid range for the GARP leave timer has been changed to 20-600 centiseconds.

- IP Multicast Static Route Configuration

  The command for configuring a static IPv4 multicast route has changed to **ip mroute**. The **ip multicast staticroute** command is deprecated.

- Support for Long User Names

  The **show users**, **show users accounts**, and **show users login-history** commands have changed. The **long** parameter has been added to these commands to support long usernames.

- Flow Control

  Flow Control is enabled by default.

  Note: When you upgrade a switch to this release, flow control is automatically enabled. If your previous configuration had flow control disabled, you must disable flow control after the upgrade to match the previous configuration.

- VLAN Limit Increases

  MAC based VLAN limit was increased from 128 to 256.
  Subnet based VLAN limit was increased from 64 to 128.

- ACL Changes

  The following changes apply to ingress and egress ACLs:

  - Maximum of 100 ACLs
  - Maximum rules per ACL are 127

  Note: Although the maximum number of ACLs is 100, and the maximum number of rules per ACL is 127, the system cannot support 100 ACLs that each has 127 rules.

  Note: Any given port can support up to 127 rules. These 127 rules can be in a single ACL or in multiple ACLs that are applied to the interface.

  Note: ACL's can be applied to all Ethernet interfaces.

Deprecated Commands and Parameters

The following CLI commands have been deprecated since the 2.x release.

Title	Description
bridge address	Interface Configuration mode Rationale: The following parameters have been deprecated: • **delete-on-reset** • **delete-on-timeout** • **secure**
ip dhcp filtering	Global Configuration mode Rationale: The **ip dhcp filtering** command has been deprecated. It has been replaced by the **ip dhcp snooping** command.
ip multicast staticroute	Global Configuration mode Rationale: The **ip multicast staticroute** command has been deprecated. It has been replaced by the **ip mroute** command.
ip dhcp filtering trust	Interface Configuration mode Rationale: The **ip dhcp filtering trust** command has been deprecated. It has been replaced by the **ip dhcp snooping trust** command.
show ip dhcp filtering	Privileged EXEC mode Rationale: The **show ip dhcp filtering** command has been deprecated. It has been replaced by the **show ip dhcp snooping** command.
mdix	Interface Configuration mode Rationale: The **mdix { auto | on }** command has been deprecated. Crossover is always automatically detected on ports.
port security	Interface Configuration mode Rationale: The following parameters have been deprecated: • **forward** • **discard-shutdown**
logging buffered size	Global Configuration mode Rationale: The **logging buffered size** command has been deprecated. The buffer size is now fixed at 400 entries.
rmon table-size history	Global Configuration mode Rationale: The **rmon table-size history** command has been deprecated. The RMON history table size is now fixed at 270.
rmon table-size log	Global Configuration mode Rationale: The **rmon table-size log** command has been deprecated. The RMON log table size is now fixed at 100.
spanning-tree bpdu filtering	Global Configuration mode Rationale: The **spanning-tree bpdu filtering** command has been deprecated. It has been replaced by the **no spanning-tree bpdu flooding** command.
MSTP Mode	MST mode Rationale: The **abort** and **show** commands in MST Configuration mode have been deprecated.

Title	Description
ip ospf	Interface Configuration mode Rationale: The **ip ospf** command has been deprecated. This functionality has been replaced by the **ip ospf area** command.
ip ospf areaid	Interface Configuration mode Rationale: The **ip ospf areaid** command has been deprecated. This functionality has been replaced by the **ip ospf area** command.
ip dhcp filtering	Global Configuration mode Rationale: The **ip dhcp filtering** command has been deprecated.
ip dhcp filtering	Interface Configuration mode Rationale: The **ip dhcp filtering trust** command has been deprecated.
show ip dhcp filtering	Privileged EXEC mode Rationale: The **show ip dhcp filtering** command has been deprecated.

Issues Resolved

The following is a list of issues resolved in the current firmware release.

Description	User Impact	Resolution
Unable to configure IPv6 host (4001::2) as an SNMP trap receiver on the DUT.	User is not aware that the only IPv4 address is accepted by the command **snmp-server host <ipaddress>** and so may try to give IPV6 address as input.	Updated the help string to mention that IPv4 address is expected as input for **snmp-server host <ipaddress>** CLI command.
WFB: Logging messages show UTC time only.	Logging messages show UTC time instead of updated time with timezone offset.	Used simAdjustedTimeGet() function for correcting log messages time.
Web: Zone config incorrect with summer time config.	Zone is not correctly populated on the web page with the summertime taken into consideration.	Added an object to get the information on summertime check and based on this value, populating the zone in the web page.
MLD Packets are not snooped, when sending MLD packets with Hop-by-Hop header with Router Alert Option.	PC6200 cannot properly identify IPv6 MLD packets that have the hop-by-hop option set like other chips such as FP2.	Added a new MLD rule to the FFP which will trap to the CPU IPv6 Membership reports which use the well known MAC address 33:33:00:00:00:16.
Firmware missing **no** command to remove **switch x priority x.**	The **no switch 2 priority 2** command does not work. There is no **no** form for	Added the **no** version of the command, setting the value to the default.
Missing RFC1213 MIB-2 SNMP Trap counter.	User could not walk all objects in SNMP group.	Re-enabled objects to provide support even though the objects were obsoleted in RFC
Member xx changes do not result in prompt to save running-config on reload.	If there is an unsaved member, standby, or NSF configuration, user is not warned of the unsaved configuration on issuing reload.	Set the unitMgrCfgFile -> dataChanged flag in the respective APIs.
Cut-through mode does not show in running-config.	The user cannot determine how cut-through mode is configured via the show running-config command.	Added a comment to the running config to indicate when the switch is configured in cut-through mode. The switch must be rebooted for the cut-through configuration to be changed.
Asset-tag is not set on stack members.	If a user would run the **show system id** on the stack member, the asset tag would not be displayed.	Process SET_ASSET_TAG event while in connected_unit/connected_stby state.
GVRP CLI vs. GUI inconsistency.	CLI and Web field names are different and used reverse to each other.	Make the Web field names similar to those of CLI such that the configuration is understood correctly.
Configured non-existing host cannot be deleted for logging syslog.	Configured non-existing host cannot be deleted for logging syslog.	Corrected logic so that only valid servers could be deleted.
Syslog server CLI description accepts invalid control characters	Validation for syslog description is different between Web and CLI.	Added validation for syslog description in CLI to accept control characters: 'a-z' | 'A-Z' | '0-9' | " " | ' @ ' | ' # ' | ' $ ' | ' _ ' | ' - ' | ' . '

Description	User Impact	Resolution
Bridge multicast forbidden forward-unregistered causes L3 Multicast to fail.	Flooding in ingress VLAN.	Modified the L3 interaction code of snooping to notify the driver when snooping is enabled. When snooping is disabled, the current operational state of snooping is also sent to the driver.
Cut-through mode command help is not clear.	For normal command and no command the help information is the same.	Changed the help information
Console logging levels help does not indicate precedence.	Help content needs to show severity level of logging.	Added the severity levels to the help strings.
Web Dot1x Authentication Max Users show units in seconds vs. # Users.	Incorrect help string added in read-only page of dot1x, causing user confusion.	Removed help string for read-only page of dot1x.
Web and CLI disagreement on Dot1x statistics.	Not displaying the MAC address correctly in the field **Last Frames Source** in the web page **EAP Statistics**.	Corrected the problem in the object handler.
ReFormatFlashFileSystem no available via the boot menu.	ReFormatFlashFileSystem cannot be executed from boot menu.	The ReFormatFlashFileSystem operation is now available via the boot menu.
Show interfaces advertise ethernet <unit> <port> command is not parsed properly.	Show interfaces advertise ethernet <unit> <port> command is not parsed properly.	Added a check for invalid interface.
Stack port link status mismatch in CLI and Web interface when configured for Ethernet.	To display the correct link status when configured stack mode is Ethernet in the Stack Port Summary web page.	Corrected the web page to properly handle Ethernet and show link status as up.
Web Home > General > Asset selection does not show details.	Incorrect link for Asset page on General Index page.	Corrected the file name for the Asset page.
Mirroring port should not send CDP packets.	Both mirrored and mirroring ports are sending CDP packets.	Get probe events, and mark interface as acquired in ISDP database. As a result, ISDP does not participate on this port.
Backups with SNMP do not work correctly.	The MIB allows users to backup the starting configuration to TFTP using SNMP, but the file is corrupted.	Corrected handling of upload filetypes and setting local filename in SNMP.
END command with all upper case is not understood by CLI.	User will not be able to go to root mode by entering END.	Use case insensitive comparison.
Trying to add ninth member to a channel-group shows LACP assignment in HTTP view.	Trying to add ninth member to a channel-group shows LACP assignment in HTTP view.	Corrected the code to enable LACP after ports are added to lag successfully.
Switchport protected name accepts non-alphanumeric characters.	Needed to check that protected port name accepts only alphanumeric characters.	Enhanced the validation.
Description inconsistency between HTTP and CLI Administration.	Spaces were not accepted in description fields through web.	Added appropriate validation.
Inconsistent CLI and Web interface responses for STP LAG settings.	Inconsistent CLI and Web interface responses for STP LAG settings.	Use the CLI formatting such that both the CLI and Web are in sync.
Ip host parse	Some ip host names with numbers and periods are rejected.	Corrected the host name checks.

Description	User Impact	Resolution
Cannot enter Daylight Saving Time from Web interface.	In summer time configuration page, in recursive mode, clock zone field is not accepting valid range.	In summer time configuration page, in recursive mode, added appropriate regular expression in validation.
Error message when changing SNTP Server Priority from Web interface.	When priority is set through Web interface for SNTP Server, and no encryption key is configured, the system returns an error message.	Upon setting the priority to SNTP server when no encryption key is configured, the key is now submitted to the switch.
Custom Protocol VLAN shows incorrect VLAN ID.	VLAN protocol group if configured for custom protocol using ethertype did not display the VLAN id in the Switching > VLAN > ProtocolGroup web page.	Made modifications to the Switching > VLAN > ProtocolGroup web page in order to resolve the issue.
NIM_events prints unknown characters.	Unknown characters being displayed are for the interface name. <190> MAY 26 05:57:54 0.0.0.0-3 NIM[99904544]: nim_events.c(603) 367 %% Component NIM generated interface event Unknown Port Event (39) for interface ?j?????? (639).	Properly initialized the variable.
VLAN protocol groups not visible in GUI.	Cannot select the protocol group on the Switching > VLAN > ProtocolGroup web page.	Display the group IDs in the list and corresponding group name below it.
Second protocol group not shown in OpenManage GUI.	In protocol-based VLAN Show All page, configured interfaces were not displayed properly. Web page affected Switching > VLAN > Protocol Group Table.	Corrected the display of the interfaces.
Adding VLAN range issues.	1. When adding a range of VLANs to VLAN Database from Web Interface, an error message is returned when no name is entered. 2. VLAN range is limited to 4 characters preventing adding certain ranges.	1. Corrected the error handling for this scenario. 2. Increased the maximum length to 250 such that a comma separated VLAN list can be configured.
Switch gives error message when entered upper case letter for interface value.	On the interface ethernet CLI command, switch gives error message when entering interface names in upper case letters.	String is converted to lower case before processing.
Custom Protocol-based VLAN does not display configurable ethertype value.	Valid range of supported ethertypes is not mentioned in CLI help.	Add supported range in CLI help.
Captive Portal login does not display error message for invalid credentials.	Captive Portal user can get confused since the login failure is not reported correctly.	Implemented logic that verifies the session state.
OpenManage Web UI shows invalid MAC address (all 0s) in ARP table.	Configuring Proxy ARP results in the ARP Table web page displaying the MAC address as all zeros.	Corrected the output of the MAC Address in the ARP Table to be the same as the Dynamic Address Table web page.
Unable to authenticate a client when radius server is given a name	User authentication does not happen when there is no default radius server.	The switch was assuming that the default named radius server will always be present. Therefore, when no default named server is present the switch will attempt to send it to the next valid radius server.

Description	User Impact	Resolution
Changing Radius Timeout from Web interface inadvertently changes Priority to same value.	Changing the Timeout Duration field on the RADIUS Server Configuration web page would also change the Priority field to the same value.	Correct the API to properly set the RADIUS priority.
Radius Servers always show active status.	The RADIUS Server Status web page was always displaying the server's status as active.	Retrieved the server status the same as the CLI for each row in the web page display.
Interface Configuration web page would not allow the user to set the MTU size to zero.	Interface Configuration web page restricted the user to configure the IP MTU from 68-9198.	Changed the weg page IP MTI field do allow the following values to be configured: 0 or 68-9198.
PCs or clients do not authenticate after reboot and logging back on (802.1x).	Windows Vista clients were not getting re-authenticated after the PC rebooted.	Modified the state machine to move to connecting state to trigger the sending of the EAP-REQ packet.
Web Display of Rapid Spanning Tree only displays first 10 interface ports	The Rapid Spanning Tree Table web page would only display the first 10, and potential incorrect interfaces.	Corrected the web page backend API to retireve all of the applicable interfaces.
Web Global Portfast applies Portfast on trunk switchports	Activating global portfast from the Web Interface applies portfast to trunk interfaces (Switching>Spanning_Tree>Global_Settings). When removing portfast globally via the CLI, it will not remove it from trunks.	While applying Portfast via the GUI, no check was present to know what the switchport access of a particular interface was hence the portfast was being applied even on trunk switchports.
IGMP Snooping failing on PC6200 stack of two switches	Two copies of DLF/Bcast/Unknown unicast packet will be sent out of the port 1 to 24 if two PC6248 switches are stacked using both the stack ports to form stack trunk.	Modified the driver layer to ignore this trunk-id while destroying external trunks.

CLI Reference Manual Updates

Non-Stop Forwarding

Title	Description
nsf ***no nsf***	Use this command to enable non-stop forwarding. The "no" form of the command will disable NSF. **Default:** Non-stop forwarding is enabled by default.
show nsf	Use this command to show the status of non-stop forwarding. **Default:** Not applicable
show checkpoint statistics	Use this command to display the statistics for the check pointing process. **Default:** Not applicable
clear checkpoint statistics	Use this command to clear the statistics of the check pointing process. **Default:** Not applicable
vlan routing vlanid [index]	This command is used to enable routing on a VLAN. Us the "no" form of the command to disable routing on a VLAN. **Default:** Routing is not enabled on any VLANs by default.
nsf [ietf] [planned-only]	Use this command to enable OSPF graceful restart. Use the "no" form of this command to disable graceful restart. • **ietf** — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional • **planned-only** — This keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the **initiate failover** command). **Default:** Graceful restart is disabled by default.
nsf helper [planned-only]	Use this command to allow OSPF to act as a helpful neighbor for a restarting router. Use the "no" form of this command to prevent OSPF from acting as a helpful neighbor. • **planned-only** — This keyword indicates that OSPF should only help a restarting router performing a planned restart. **Default:** OSPF may act as a helpful neighbor for both planned an unplanned restarts.
nsf [ietf] helper strict-lsa-checking **no nsf [ietf] helper strict-lsa-checking**	This command is used to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs. Use the "no" form of this command to allow OSPF to continue as a helpful neighbor in spite of topology changes. Default: A helpful neighbor exits helper mode upon a topology change.
nsf [ietf] restart-interval *seconds*	Use this command to configure the length of the grace period on the restarting router. Use the "no" form of this command to revert the grace period to its default. • **ietf** — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional. • *seconds* — The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The restarting router includes the restart interval in its grace LSAs (range 1 – 1800 seconds). **Default:** The default restart interval is 120 seconds.
show ip ospf	This command has been enhanced to lists the values of the configuration parameters described above and the status parameters defined in the RFC 4750 MIB.

Title	Description
show ip ospf neighbor	This command has been enhanced to list the per neighbor graceful restart status described in the RFC 4750 MIB. Possible values for Restart Helper Status are as follows: • Helping – This router is acting as a helpful neighbor to this neighbor. • Not Helping – This router is not a helpful neighbor at this time.

Port Configuration Show Command

Title	Description
show interfaces detail {ethernet interface | **port-channel** port-channel-number}	A new single command that shows VLAN, STP, Port status, and Port Configuration information. **Default:** Not applicable

Custom Protocol Based VLANs

Title	Description
vlan protocol group add protocol <groupid> **ethertype** <value> **no vlan protocol group add protocol <**groupid> **ethertype** <value>	Previously only ARP, IP and IPX are configurable as protocols for protocol-based VLANs. This has been extended so that any Ethertype may be used. • groupid—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command. • ethertype—The protocol you want to add. The ethertype can be any valid hexadecimal number in the range 1536 to 65535. **Default:** Not applicable
vlan protocol group <groupid> **no vlan protocol group <**groupid>	If the user creates multiple vlan protocol groups, deletes one of them, and then saves the configuration, the older implementation of this command resulted incorrectly applying the groupids on reload. Hence, the existing command **vlan protocol group <**groupname> is updated to **vlan protocol group** <groupid> so that groupid is used for both configuration and script generation. • groupid—The protocol-based VLAN group ID, to create a protocol-based VLAN group. To see the created protocol groups, use the **show port protocol all** command. **Default:** Not applicable
vlan protocol group name <groupid> <groupName> **no vlan protocol group name <**groupid>	This is a new command for assigning a group name to vlan protocol group id. • groupid—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command • groupName—The group name you want to add. The group name can be up to 16 characters length. It can be any valid alpha numeric characters. **Default:** Not applicable

VLAN Name Support with RADIUS Server

Title	Description
show dot1x Ethernet *interface*	The command was updated to display the VLAN Id, or name as required. **Default:** Not applicable

RADIUS Accounting Servers

Title	Description
radius-server host acct	The switches do not support creating accounting server names with the same name although the CLI Reference Manual and User Guide state that it is supported. **Default:** Not applicable

Spanning Tree

Title	Description
no spanning-tree transmit hold-count	The hold-count keyword is not required when resetting the spanning-tree transmit hold-count. **Default:** Not applicable

Stacking/CX-4 Module Configuration

Title	Description
stack-port <unit>/<port-type> <port-num> {ethernet | stack}	This command is used to configure a port on a CX-4 or stacking plug-in modules as either an ethernet or stack port. **Default:** From the factory the ports are all configured as Ethernet ports. If upgrading from a previous release the modes will be preserved and no configuration should be necessary.

Configurable Message of the Day Banner

Title	Description
banner motd <message> **no banner motd**	Controls (enables or disables) the display of message-of-the-day banners. 'banner motd' enables the banner, and allows configuration of message-of-the-day banners. Use 'no banner motd' to delete the message, and disable the banner. **Default:** Disabled by default.
banner motd acknowledge **no banner motd acknowledge**	The user will be required to acknowledge the banner displayed on the console if 'banner motd acknowledge' is executed. The user would have to type "y" or "n" to continue to the login prompt. If "n" is typed, the session is terminated and no further communication is allowed on that session. However, serial connection will not get terminated if user does not enter 'y'. Use 'no' form of the command to disable banner acknowledge. **Default:** Disabled by default.

Dot1X

Title	Description
dot1x timeout guest-vlan-period	Use this command in Interface Config Mode to set the number of seconds that the switch waits before authorizing the client if the client is a dot1x unaware client. **Default:** The switch remains in the quiet state for 90 seconds. Refer to the *Dell™ PowerConnect™ 6200 Series Systems CLI Reference Guide* for details.

Link Dependency Commands

Title	Description
link-dependency group [action { **up** | **down** }]	Use the action command to control the operational state of the group based on the dependent links state. • **up** — Causes the group members to change their operational state to be opposite that of the dependent link. • **down** — Causes the group members to change their operational state to follow that of the dependent link. **Default:** Not applicable.

Multicast

Title	Description
ip pimdm mode **ip pimdm query-interval** **show ip pimdm interface**	PIM-DM commands not supported in the 3.2 release are documented in the CLI Reference Manual.

User's Guide Updates

Configuring Dell PowerConnect

Title	Description
User's Guide	See: Dell™ PowerConnect™ 6200 Series User's Guide
Configuration Guide	See: Dell™ PowerConnect™ 6200 Series Configuration Guide

Known Issues

Summary	User Impact	Workaround
Non-configuration file getting loaded to startup-config through HTTP.	When the switch reboots and attempts to read an invalid start-up configuration file, it will give up and create a default startup configuration.	It is recommended that all users keep backups of their configuration files.
TACACS operation	User cannot enter Privileged EXEC mode without using the **enable** command.	None.
Ping fails with 33% to 100% packet loss	Using a Windows 7 client and pinging with a 59900 byte packet will result in packet loss.	None.
OSPF Dead interval expires on neighbor, when the DUT stack manager restarts with *large* configuration.	In a large stack with an unusually large configuration, it is possible that during an unplanned failover, the control plane may not issue OSPF grace LSAs before the dead interval expires on neighbors. When this happens, neighbors report the router down and other routers in the area recomputed OSPF routes to avoid the restarting order.	Increase the dead internal timer.
VLAN configuration is not successful on ports after detaching them from LAG.	The issue is that any VLAN configuration applied to a physical port while it is a member of a LAG will not be applied when the port leaves the LAG.	This is not a problem if VLAN configuration is performed while the port is not a member of a LAG. If the configuration is saved and the switch is reset, the configuration is applied correctly.
Issue with PBVLAN configuration migration.	The command vlan protocol group expected a string in earlier versions; now it expects a number.	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 is getting 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 this local user access level (Read-write or Read-only).
TFTP gives no reason for file download failures.	Generic failure message.	None.
CLI command stack-port config rejection does not display the cause.	If a user enters an invalid interface, a generic error message will be generated: ERROR: Invalid input.	None.
Banner MOTD: The switches Console and Web sessions are inaccessible until the user acknowledges the banner of the day.	The current implementation of the MOTD acknowledgement results in all user interface sessions being inaccessible until the user enters a response or the 30-second timeout occurs. While the acknowledge process is pending, it cannot process the other UI sessions. Once the timeout occurs, then the MOTD acknowledgement ends the connection and resumes processing of the other sessions.	Acknowledge the message to avoid the session timeout.
DHCP server has data changed flag set after booting from saved config.	If DHCP server is enabled, then the user may be prompted to save configuration changes even though no configuration changes have been made.	None.

Summary	User Impact	Workaround
Bridge multicast address is shown as MAC Address format in **show running-config** buffer when it is configured in IP format.	If a user configures the bridge multicast address as an IP address format in VLAN interface mode, it is displayed in the show running-config command in MAC address format.	None.
Connected spanning tree root port role not changed to auto-portfast after disabling MSTP on Trunk.	A port that is a root port will not become auto edge port if the bridge that the root port is connected to goes away.	This means that the port would flush the Forwarding Database entries every time that there is a topology change. This could be avoided if the link goes down and comes back up.
Three commands are not available at interface range Ethernet level, but are available at interface.	The following commands are not available to use in interface range Ethernet level: isdp, lacpa, and protocol.	Each interface must be configured individually.
There is no command to add protocol vlan in interface range mode.	The user cannot use interface ranges to configure a protocol VLAN.	Each protocol VLAN must be configured individually.
Invalid error port number displayed on log message when VLAN is changed to forbidden mode from access mode.	When port is changed to forbidden mode from access mode, the log message below is generated that reports the wrong port number. <187> OCT 12 08:39:03 10.131.6.173-1 DOT1Q[104741168]: dot1q_api.c(525) 2475 %% Port(88) This log message is correct when a port from the base unit is selected.	None.
Gratuitous ARP packets are not being generated when management VLAN is changed with static IP configuration.	If the user changes the management VLAN, then management connections must be re-established on the new VLAN. Neighbors will resolve the switch's management IP address on the new VLAN.	None.
Using interface range mode not able to configure protected ports.	Cannot use interface range mode to configure protected switchports.	The user must configure each protected port individually.
TFTP fails to display specific error message when incorrect filename was given while downloading the code.	If a user attempts to tftp a non-existent file to the image of the switch, nothing will be downloaded and there will not be an error message generated.	None.
Web needs to provide an option to configure sFlow sampler / poller values on range of interfaces.	User will not be able to select range of interfaces through web for the Sampler and Poll Configuration web pages. However, configuration is not affected as user can individually select the interfaces and configure.	User has to select each interface individually to configure in the Sampler Configuration and Poll Configuration web pages.

Summary	User Impact	Workaround
ISDP updates are not including Voice VLAN Reply TLV when Voice VLAN ID on interface is changed.	Upon changing configuration immediately after getting the VLAN assigned, DUT stops advertising Voice VLAN reply TLV in its ISDP updates which causes IP phone to change its VLAN properties.	The administrator can work around this problem by shutting down the port and restarting it after the configuration is changed.
PC6200 fails to re-authorize IP phone upon enabling and disabling Voice VLAN authentication.	Once a phone is configured, enable Voice VLAN authentication, wait for DHCP discovery again, and then disable Voice VLAN authorization. On disabling Voice VLAN authorization, PC6200 fails to authorize IP phone based on the received LLDP packet (with network policy TLV).	Disconnect and reconnect the phone to the port, the phone gets authorized.
When Line or enable method is used as login method and enable authentication is none, the user is unable to enter into Privileged EXEC mode.	If login authentication method is Line or Enable, and enable authentication is None, you will always get read-only access (because there is no user configured for line or enable authentication). The user will never get read-write access.	If enable authorization is set to None, ensure that the login authorization method is at least TACACS, Radius, or Local. Any authentication method that requires a user configuration will ensure that the user will get proper access based on how the user is configured.
Cannot change LAG mode from Static to Dynamic via CLI.	Cannot change LAG mode from Static to Dynamic via CLI.	The user may change the LACP Mode using the Graphical User Interface.

Known Restrictions and Limitations

Layer 2

802.1AB (LLDP)

Description	User Impact
LLDP-MED location and inventory transmit TLVs have no effect.	The switch does not support configuring this data so enabling these TLVs has no effect.

QoS

Description	User Impact
Traffic permitted by an outbound ACL on one port can be allowed on another port.	This behavior is a limitation of implementing egress ACLs on an ingress classifier. Given a configuration where two outbound ACLs are active on different ports. Since both ACLs are applied in the 'out' direction, the rules programmed into the IFP will match on any ingress port. Ultimately, w/ the implementation of egress ACLs on the ingress classifier, unexpected behavior occurs if overlapping rules (i.e. a given packet can match multiple rules) are applied to different ports in the outbound direction.
Ip-dscp-mapping is not working as per the configured priority Queues on 10G (CX4) ports.	This is only an issue when forwarding traffic between 10G interfaces on different switches in a stack. The stack link can only support 12G so if it is oversubscribed, the effects of the queues are reduced.

802.1X

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**.

LACP

Description	User Impact
LAGs Supported	Number of LAGs supported: • Up to 18 Dynamic LAGs • 48 Static LAGs Limitations (stack of 12) • Long Timeouts With a minimal CPU load, it takes approximately 1.5 minutes with 16 dynamic LAGs and 15 MSTP instances for the ports to become active with traffic running. • Short Timeouts With a minimal CPU load, it takes approximately 1.5 minutes with 12 dynamic LAGs and 15 MSTP instances for the ports to become active with traffic running.

VLAN

Description	User Impact
vlan association mac command limitations	The maximum number of MAC-based VLANs is 256.

Layer 3

IP Map

Description	User Impact
ip default gateway and **ip default route** are for different types of interfaces. **ip default gateway** is for the management interface and **ip default route** is for VLAN routing interfaces.	Ensure the correct command is used for the interface being configured.

DiffServ

Description	User Impact
Failed to attach diffserv policy to an interface with **mark cos** and **assign queue** attributes.	This behavior is a known limitation of the PowerConnect 6200 series switches.

ICMP

Description	User Impact
IPv4 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). This is a hardware limitation and is working as designed. The HW does not allow the IP MTU to be configured per VLAN. We can configure the maximum frame size in HW using the 'mtu' command in interface Ethernet mode. However, if a packet exceeds the maximum frame size for a port, it is discarded. If a packet happens to be sent to the software and it exceeds the IP MTU, then the packet still will not be fragmented. An ICMP error message is sent to the sender.
ICMP Error message generation	The ICMP Error Message generated by the switch has the fields (TTL) unmodified instead of sending with a modified value resulted as a part of forwarding process.
ICMPv6 Packet Too Big	The system is not generating Packet Too Big message to the source when it forwards the packet through an interface vlan with mtu smaller than the packet being forwarded. The PowerConnect 6200 Series switches do not have the capability to enforce IP MTU on VLAN Routing interfaces..

Multicast

Description	User Impact
Multicast VLC streams are not received on VLC client on complex network topology.	This is not a mainstream problem. DVMRP functionality works fine and such issues are not seen in 2 or 3 router topologies. This issue is seen only in complex topologies under high loads in the presence of other multicast entries upon table full conditions.

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 and add it back.

SNMP

Description	User Impact
Not able to set the value for dellLanMngInfEnable	Management ACLs are always enabled and cannot be disabled.
dot3StatsAlignmentErrors not incrementing	The value for all ports shows up as 0.
agentInventoryStackReplicateSTK object not working as expected	Copies backup image of master to member instead of active image of master.
agentStpPortRootGuard object	Use agentStpCstPortRootGuard instead.

Web-based Management

Description	User Impact
Traffic Monitoring Chart Rate Display	The chart displays a count rather than a rate.
Stacking Ports displayed on the LLDP, LLDP-MED, and Voice VLAN configuration pages	The interface selections available on the configuration pages contain the stacking ports which are not applicable.
Browser-specific issue: On the VRRP Router Configuration page, the authentication type is not saved when using Firefox v2.x.	To configure the authentication type, either upgrade the browser to Firefox 3.x or use the CLI.

Cable Diagnostics

Description	User Impact
Cable Length Diagnostic shows result as 'Unknown' for a port to which Network is connected.	Problem is intermittent and only observable when connected to a D-Link DES1008.

File Management

Description	User Impact
Error displayed on console while applying configuration for a 48 port switch to a 24 port switch.	When applying configuration to ports which do not exist, errors are generated such that all subsequent commands fail. User Action: Remove the configuration for the non-existent ports.
CLI Comment Character	The '!' indicates the beginning of a comment. All characters following the '!' will be treated as a comment.

End of Release Notes