

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

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



**Date: January 2011**  
**System Firmware Version 3.2.1.3**

**Information in this document is subject to change without notice.**

**© 2003 – 2011 Dell Inc. All rights reserved.**

Reproduction in any manner whatsoever without the written permission of Dell Inc is strictly forbidden.

Trademarks used in this text: Dell, the DELL logo and PowerConnect are trademarks of Dell Inc; Intel and Pentium are registered trademarks and Celeron is a trademark of Intel Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entity claiming the marks and names or their products. Dell Inc disclaims any proprietary interest in trademarks and trade names other than its own. All rights reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without the prior written consent of Dell. Dell reserves the right to make changes without further notices to any products or specifications referred to herein to improve reliability, functionality or design.

Reproduction, adaptation or translation without prior written permission is prohibited, except as allowed under the copyright laws.

## *Table of Contents*

<b>Introduction</b>	<b>1</b>
<b>Global Support</b>	<b>1</b>
<b>Firmware Specifications</b>	<b>1</b>
<b>Hardware Supported</b>	<b>3</b>
<b>Added Functionality in this Release</b>	<b>4</b>
Release 3.2.1.3	4
Release 3.2.0.10	4
Release 3.2.0.9	4
Release 3.2.0.7	4
<b>Changed Functionality in this Release</b>	<b>17</b>
Release 3.2.1.3	17
Release 3.2.0.10	17
Release 3.2.0.9	17
Release 3.2.0.7	17
<b>Issues Resolved</b>	<b>23</b>
Release 3.2.1.3	23
Release 3.2.0.10	24
Release 3.2.0.9	24
Release 3.2.0.7	25

<b>Deprecated Commands and Parameters</b>	<b>36</b>
<b>CLI Reference Manual Updates</b>	<b>39</b>
<b>User's Guide Updates</b>	<b>45</b>
<b>Known Issues</b>	<b>46</b>
Release 3.2.0.10	46
Release 3.2.0.9	46
Release 3.2.0.7	47
<b>Known Restrictions and Limitations</b>	<b>51</b>
<b>Layer 2</b>	<b>51</b>
<b>Layer 3</b>	<b>52</b>
<b>Management</b>	<b>54</b>
<b>End of Release Notes</b>	<b>55</b>



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

## Introduction

This document provides specific information for the Dell PowerConnect 6200 Series switches, firmware version 3.2.1.3.

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	3.2.1.3	January 2011

### 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
PC6200v3.2.1.3.stk	3.2.1.3	January 2011

Version Numbering Convention					
Version number				Description	
6200 Series	3	2	1	3	Four part version number
				t	Denotes the build number.
			t		Denotes an ad hoc release of the product software.
		t			Denotes a scheduled maintenance release of the product software.
	t				Denotes a major version number.

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

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

## Hardware Supported

PowerConnect 6224

PowerConnect 6248

PowerConnect 6224F

PowerConnect 6224P

PowerConnect 6248P

## Added Functionality in this Release

### Release 3.2.1.3

#### ➤ Auto Detect and Configure Ports for iSCSI Traffic

The iSCSI component, when enabled via the *iSCSI enable* command, registers with the LLDP component to receive notification of the appearance and withdrawal of Dell Equal Logic (EQL) arrays, specifying the EQL System Description in the registration. This feature only works when the EQL arrays have software version 5.0.2 or later installed and running.

Upon iSCSI being enabled, the following actions occur:

- A detailed warning message is issued indicating the automatic changes that will occur (globally enabling jumbo frames, mtu set to 9216, as well as the spanning-tree portfast settings that will occur when EQL array is detected).
- Flow control is globally enabled if not already enabled.
- MTU 9216 is enabled on all ports and port-channels.

Upon receipt of an EQL appearance notification, the iSCSI component will configure the ports as follows:

- spanning-tree portfast is enabled on the interface identified by LLDP
- unicast storm control is disabled on the interface identified by LLDP

Upon receipt of an EQL withdrawal notification, no action is taken.

### Release 3.2.0.10

No new features introduced in Release 3.2.0.10.

### Release 3.2.0.9

No new features introduced in Release 3.2.0.9.

### Release 3.2.0.7

#### ➤ 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.

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

## ➤ 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

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

## 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

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

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/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.

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

## ➤ 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.

➤ OSPFv2/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.

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

## ➤ 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

### Release 3.2.1.3

No changed functionality in Release 3.2.1.3

### Release 3.2.0.10

#### ➤ Temperature Threshold

The CPU and temperature LED temperature threshold has been changed from 45C to 57C. This temperature change prevents erroneous temperature alerts when in use in high altitudes and high temperature environments.

### Release 3.2.0.9

No changed functionality in Release 3.2.0.9

### Release 3.2.0.7

#### ➤ Diagnostically Disabled port

A port can be put into the disabled state for the following reason:

- Spanning-Tree: If STP BPDUs are received at a rate of 15pps or greater for 3 consecutive seconds on a port, that port will be diagnostically disabled..
- DHCP Snooping: If DHCP packets are received on a port at a rate that exceeds the threshold for a specified time, that port will be diagnostically disabled. The threshold is configurable up to 300pps and the burst is configurable up to 15s long. Default is disabled.
- Dynamic ARP Inspection: If Dynamic ARP Inspection packets are received on a port at a rate that exceeds the threshold for a specified time, that port will be diagnostically disabled. The threshold is configurable up to 300pps and the burst is configurable up to 15s long. Default is 15pps and 1s burst.

#### ➤ 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

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

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

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

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.

➤ Port Speed with Negotiation Disabled

Ports no longer default to 1G when negotiation is turned off. It is also no longer possible to force 1G speeds since auto-negotiation is required for that speed to work.

## Issues Resolved

### Release 3.2.1.3

Description	User Impact	Resolution
Link Status should be displayed as D-Disable instead of Down, when a BPDU Guard enabled port receives BPDU with a higher priority.	The incorrect link status will be reported.	The status was updated to reflect the proper state of the port.
Spanning-Tree BPDUs are being flooded even though status screen show BPDU flood disabled.	Spanning-Tree BPDUs might still be flooding even though the status says that flooding is disabled.	The Spanning-Tree BPDU flooding status is displayed correctly on the status screen.
Switch occasionally hangs on reload.	User may experience hangs which require a reboot.	Corrected a problem with a semaphore that was not being released properly before it was being acquired again.
Hostname is not updated in Running-Config when the name contains periods '.'	The previous hostname is still used.	Check was incorporated so that all printable characters may be used.
Probe port is not dropping the traffic when a port mirror session is enabled.	Traffic will get inadvertently switched to the device connected to the probe port when it should not.	Delete the L2 entry that is associated with the probed port.
Fatal error crash and reload when uplinked to Cisco 6509 with ISDP enabled.	The switch will crash and reboot as long as the cable is connected.	Fixed an internal buffer size mismatch.
Displaying the wrong LACP system MAC address in "show lacp port-channel".	The incorrect MAC address was shown for the partner switch in "show lacp port-channel" cli command output.	Corrected the logic that retrieved the MAC address.
Console Lockup while configuring ACL for Dynamic ARP Inspection (DAI).	The console will lockup while configuring ACL for DAI.	Corrected logic that was causing a semaphore deadlock.
Combo ports 1/g45 - 1/g48 do not pass traffic when no negotiation is set	After ports 1/g45-1/g48 are configured with no negotiation set, when the switch is reloaded the ports do not pass traffic.	Corrected logic that caused the internal and external PHY drivers to get out of synchronization
HTTPS fails if HTTP is disabled.	HTTPS becomes inaccessible after switch reboot if HTTP is disabled and HTTPS is enabled.	Corrected logic that failed when the HTTPS socket was being bound.
The status of VLAN 1 routing interface becomes DOWN	VLAN routing interface is down while there is an active physical interface which includes the VLAN.	Corrected the notification that is used to determine the state of the VLAN.
Ports 1 & 2 on a 24 port switch are not operational on MEMBER switch.	If no cable is plugged into ports 1, 2 on a 24 port switch when the stack is reloaded ports 1, 2 are not operational. If a cable is plugged in the port initializes correctly.	Corrected the timing issue associated with bringing the PHY out of reset for those ports.

Description	User Impact	Resolution
Ports 25 & 26 on a 48 port switch are not operational on MEMBER switch.	If no cable is plugged in to ports 25 or 26 when the stack is reloaded ports 25 or 26 are not operational. If a cable is plugged in the port initializes correctly.	Corrected the timing issue associated with bringing the PHY out of reset for those ports.
When using TACACS to authenticate user access to switch management AND a Management ACL is applied, no user login attempt is performed.	TACACS server logs show no authentication attempt when user enters switch login credentials..	Corrected the Management ACL component to proper handle the service type NONE.
IPv6 Router solicitation packet causes a crash.	The switch crashes if an IPv6 router solicitation packet is received if IPv6 is not enabled.	Check for IPv6 being enabled before handling IPv6 solicitation packets.
Switch crashed when the port for the default route is disconnected.	The switch crashes when the default route is removed from the routing table.	Corrected the failure condition when an attempt is made to traverse the radix tree with the default route.

## Release 3.2.0.10

Description	User Impact	Resolution
Local Proxy ARP is being set enabled as the default when using the Web Interface.	Local Proxy ARP should be disabled by default.	Change the initial value of that configuration item to disabled in the web initialization parameters.
LACP not working with Juniper EX-4200 when supporting Non-Stop Forwarding	The LAG will not establish because all the LACP data units are dropped.	Dropped LACP data units were caused by an incorrect packet length. The packet length of 132 was changed to 128 in order to conform to the standard.

## Release 3.2.0.9

Description	User Impact	Resolution
When a stack member is reloaded and brought back up, the unit re-joined the stack but the hosts connected to it were inaccessible.	Member unit not forwarding traffic after a reload. The stack must be reloaded to recover.	Changed the behavior of sending unauthorized events to all link down ports and authorized events again on link up to eliminate timing dependencies.

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

Description	User Impact	Resolution
When bringing a failed former Master unit back online, a LAG distributed across the two stack members will drop all traffic for up-to 40 seconds.	This is a problem in static LAGs where the remote end will attempt to transfer data down the link which will be dropped until full port initialization occurs which takes approximately 40-60 seconds after reboot.	Modified the boot and application code to minimize the port initialization time between hardware power up and software initialization.
SNMP goes unresponsive after long periods of high frequency polling.	The switches will stop responding to SNMP requests.	A semaphore now used to properly control SNMP and CLI access to common configuration data structures.
PC62xx switches only send LLDP packets to root port when they are not root.	If an interface is part of a port-channel, it does not transmit LLDP frames.	Corrected behavior such that LLDP is no longer affected by the DOT1s state of the port.
EAP Requests were not being sent after the Quiet period time out.	EAP Requests are NOT sent.	Corrected logic in connecting action if the previous state was held or abort.
Packets that are greater than 1518 bytes, when transmitted through a LAG, are counted as packet errors.	LAG error statistics are not correct.	Corrected the parameters that identify LAG large packet errors.
Some of the static routes that have been redistributed into OSPF are not seen in neighbor routers routing table, they are however in the OSPF database.	OSPF may not compute routes for some external LSAs if the LSA specifies a non-zero forwarding address. This could also cause OSPF virtual links to not come up.	Modified the way the OSPF trees are built and traversed so that correct information can be extracted.

### Release 3.2.0.7

Description	User Impact	Resolution
Dot1x user re-authentication	Dot1x users do not need to re-authenticate after a switch reboot.	Corrected the 802.1X state machine.
Switch stack of 10 fails with unit # 7 present	Renumber switches with unit #7 present may cause stack split.	The updated driver code does not have this problem.
Error 0 on boot-up	This message is an artifact of events logged in previous releases. Upon boot-up, the saved events are displayed. This error message is only seen when the last booted image is from a release prior to 3.0.	The event is not generated in release 3.0.
Protect Boot Sector blocks	Boot code may become corrupted resulting in switch becoming not bootable.	The boot code sector in flash is locked except when updating the boot code.

Description	User Impact	Resolution
SFP and XFP report incorrect optical power	Inaccurate information or wrong units may be displayed.	The optical power is now displayed in dbm instead of mW.
Spanning Tree Forward Delay Timer configuration can be lost	User may have to manually add back configuration of forward delay timer after reboot.	Synchronized queues so that the timer is configured correctly.
HTTPS fails to connect from browser	Switch may crash or reject HTTPS connections.	Fixed buffer overflow bug.
Change show interface status to indicate flow control state	User cannot tell if flow control is active, on if it is configured.	Flow control status is now displayed.
Show Running Config does not show areaid for loopback interfaces	Running config shows the operational areaid instead of configured areaid. Since the interface mode is not enabled the operation areaid remains 0 and will not be shown in the running config.	The configured areaid can now be seen in the output of "show running-config".
Missing ip domain name max length in help	User is not informed the maximum length of a domain name.	The help text for this command will now show the maximum number of characters which may be used for a domain name.
Err msg when executing "show ipv6 vlan" command	User sees an invalid error indication if there are no active IPv6 addresses on an interface.	Removed bogus "err" message.
"show bridge address-table ?" describes "count" as "count"	Help text is not helpful.	Help string has been modified to explain what "count" is.
Switch crashes by just issuing show dir command	If a script file exists with a filename longer than 21 characters, the switch can crash when issuing the "show dir" command.	Corrected code to handle the maximum length file name.
dtllpv6NeighEntryDelete() : DTL arp entry count out of sync	User could see spurious warning messages.	Removed deprecated messages.
Authenticated Users not listed in MIB table	Web users could not be seen by walking the agentLoginSession table.	All users, including web users, can now be seen by walking the table.
SNTP time synchronization fails with DOSCONTROL L4PORT enabled.	Unicast SNTP traffic to the switch is blocked.	Changed unicast SNTP traffic so that it is no longer blocked.
Dropped packets counter always zero	The counters were not functional so the user could not see how many packets were dropped.	The counter is now operational.
syslog server is displaying hostname for IP address	User could not see the configured syslog host name.	The output of the <b>show syslog-servers</b> command now shows what was configured.
XFP trap messages on console are incorrect	Misleading log messages	The correct message is now displayed.

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

Description	User Impact	Resolution
Errors seen using CLI to set http/https authentication methods	Incorrect indications that the "enable" and "line" authentication methods are supported for http.	Only valid authentication methods are selectable.
no nego on gig ports	The switch appears to support 1G port speeds with auto-negotiation turned off.	Ports no longer default to 1G when negotiation is turned off. It is also no longer possible to force 1G speeds since auto-negotiation is required for that speed to work.
double vlan settings: port channel interfaces missing	User must configure double VLAN settings for port-channels from the CLI.	Redesigned web page so that port-channels can be configured via the web.
CDP (ISDP) is active on port-channels instead of the member ethernet interfaces	Incorrectly showing LAG interfaces in CLI "show isdp interface all".	Removed LAG_INTERFACE as valid interface type in ISDP interface.
Spanning-tree blocks egress of local CDP (ISDP) packets	Incorrectly stopping & restarting transmitting of ISDP packets whenever STP based active and inactive events are received. Locally generated CDP packets are blocked from egress by spanning-tree port states.	Removed active and inactive event handling.
No ISDP enable doesn't stop CDP traffic on the given port	Cannot stop CDP traffic on a port without disabling ISDP for the switch.	Removed LAG_INTERFACE as valid interface type in ISDP interface.
EU Summertime rule is not correct	Summertime in the EU starts on the last Sunday of March at 02:00 and ends on the last Sunday of October at 03:00. We presently set to start first Sunday of Mar at 01:00 and ends on last Sunday of Oct at 01:00.	Corrected summertime in the EU as it starts on the last Sunday of March at 02:00 and ends on the last Sunday of October at 03:00.
Issues with "show fiber-ports optical-transceiver" output	Customer is seeing same diagnostics for both port up and down. There are also corrupt values shown in power out.	Removed the link scan disabling and enabling and introduced a check such that we will calibrate the power only when the port is not administratively disabled. In this case we will show -40dbmw which is the absolute minimum value.
Incorrect handling of queue empty scenarios for Spanning Tree state change callbacks	All ports become DIAG-DISABLED.	Check if event queue is empty when timer fires so that head pointer is not advanced beyond tail pointer.
Time is reported as UTC and not local time	"show copper-ports tdr" shows UTC in date not in local time.	Updating time with Local time instead of UTC.

Description	User Impact	Resolution
DHCP Snooping's D-DISABLE is not working on LAGs	DHCP Snooping's rate limiting is not disabling properly on LAGs.	Disabled the rate limiting feature of DHCP Snooping by default. Incremented the HW metering parameters for DHCP Snooping flows. Corrected the set admin state function to handle the LAGs.
IGMP not working	Functionality does not work if "bridge multicast forbidden forward-unregistered" is applied before "bridge multicast filtering".	Error is thrown when "bridge multicast forbidden forward-unregistered" is enabled before "bridge multicast filtering" and for the related commands.
Problem with logging in with simple config	When radius server does not exist and the authentication fails, the next method is not getting invoked	The authentication is passing to next method and user is able to login on console.
Multiple Issues: - PC62xx SNMP walk causes switch to crash and reboot - System Uptime object stops responding to SNMP requests.	Box reboots when doing the SNMP walk.	Cleanup operation with every invocation of affected functions.
Make SNTP clock synchronized log debug level.	Log can fill up with informational message of SNTP: system clock synchronized.	Log message is now NTP debug level.
Upgrading to 3.0.0.8 causes the switch to be inaccessible via serial	Updating boot code with active file I/O has the potential to corrupt the file system or file during boot code upgrade.	Modified update boot code command to write a file to signal the bootrom to perform the update on the next reset. Modified the bootrom check for the existence of this file and perform the update automatically.
Check for invalid file descriptor in osapiFsClose	TFFS file system getting corrupted.	Prevent using invalid descriptors the OS API.
Loss of Management within a Stack	The stack may become unmanageable after 24 hours when the stack is configured as a layer 3 device. May also become unmanageable when the stack or a member unit is rebooted.	Properly return an error condition from the driver to prevent the loss of management in a stack.
After move-mgmt, the default H/W STP state for all the ports is set to forwarding	Temporary loops after move-management.	Driver explicitly sets the port spanning-tree state to disabled during initialization or reset after move-mgmt.
The CLI command "show interface status" does not recognize the admin state of DIAG-DISABLED. It simply indicates up/down	The only method to determine whether a port has been diag-disabled is to use show tech-support or see the LOG_MSG.	Check the Admin state and if DIAG-DISABLED, indicate the port is down due to a limited amount of space on the status line.

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

Description	User Impact	Resolution
PoE port power limits are too high	Power limit for ports raised from 15.2W to 20W	Revert port power limit to previous value.
Crashes seen when 802.1x enabled in a stacked environment.	Stacked switches may have stability issues if using 802.1X.	Corrected usage of semaphore.
Cable diagnostics for copper SFP missing	Cannot perform cable diagnostics on copper SFPs.	Relaxed the restrictions on which ports may run cable diagnostics.
Blocked STP ports will not show in the "show spanning-tree blockedports" output	User cannot tell if a port has been blocked because a BPDU has been received.	The port is set to discarding state.
Ping times vary widely	When pinging an interface on the switch, the ping response times can vary widely.	Improved the efficiency and scheduling of the background system information task.
IS-IS traffic on a tagged VLAN is not forwarded properly	Unless the IS-IS traffic is on the default VLAN, it will not be forwarded correctly.	IS-IS traffic is now sent with the correct egress VLAN tagging.
In certain topologies, L2 Multicast traffic is not flooded in a VLAN	Only L3 forwarding of Multicast traffic is performed.	Corrected the IP Multicast VLAN pruning procedure.
Unable to delete an IP Helper address without a port number.	From the CLI, an IP Helper IP address cannot be deleted without specifying a UDP port.	Corrected the CLI tree to allow this command format.
IGMP Snooping accepts invalid join requests	Join requests with a TTL greater than one should be dropped. IGMP does but IGMP Snooping does not.	Corrected IGMP Snooping to drop joins with a TTL greater than one.
ROVR errors on stack ports	ROVR errors are observed on a correctly functioning stack port.	Correct the maximum packet size allowed on stack ports so that the counter is accurate.
Connected phones may fail to connect or have multiple LLDP entries.	Phone will not reliably connect to the network upon booting.	Ensure that source MAC address is used to uniquely identify each LLDP station.
DHCP Snooping can create a loop using ports in discarding state.	DHCP will run slower and slower.	Discard DHCP packets if a port is not forwarding.
SNMP can crash under heavy load.	If the switch is being hit with lots of SNMP and RMON traffic, it can crash.	SNMP and RMON access some common data so access to the data is now serialized.
MAC addresses of authenticated 802.1X supplicants do not appear in the bridge address table.	The MAC addresses of the supplicants cannot be seen.	Ensure that the MAC addresses appear in the bridge address table.
IGMP Querier does not work if IP Multicast not enabled.	User must enable IP multicast in order for IGMP Querier to work.	Automatically enable IP Multicast when IGMP is enabled.
DHCP packets are not seen by 802.1X so clients are not able to be authenticated.	802.1X unaware clients that send only DHCP packets may not get authenticated using mac-based authentication.	Ensure that the DHCP packets from the unauthenticated client are passed to 802.1X so the client can be placed in the guest VLAN.

Description	User Impact	Resolution
"Available Memory" as reported by the web interface is wrong.	The available memory is multiplied by 1024.	Removed the multiplication factor so that the memory is reported correctly.
DOS Control ICMP packet size includes the header	User must add the size of the ICMP header (8 bytes) to the DOS Control command.	Changed the <b>dos-control</b> command so that the ICMP packet size refers to the payload only.
VLAN 1 (default VLAN) automatically added to switchport mode general ports.	After removing VLAN 1 from a port, saving the config and rebooting, VLAN 1 will once again be participating on the port.	Stopped inappropriately adding VLAN 1 to ports.
IP Multicast and LAGs can cause the switch to crash.	Heavy IPv4 Multicast traffic can cause a crash in certain situations.	Stopped contention in the driver between IP Multicast and LAGs.
Switch can crash while moving the manager if bridge multicast filtering is configured.	Once in this state, the switch will crash repeatedly until the configuration is cleared.	Validate the interfaces used by bridge multicast filtering.
Switch may reboot if certain DNS options are present in the DHCP options.	Switch may reboot upon completion of system initialization.	Ensure that the DNS is ready to receive the options.
Switch may crash if unit 12 is a 6248.	Moving the manager may cause the switch to crash if unit 12 is a 6248.	Corrected the access to the highest numbered port.
File name longer than 256 characters causes crash.	Listing the files on the switch file system can cause a crash if there is a file name which is too long.	Hardened the code to gracefully handle a ridiculously long file name.
SSH sessions can be confused during key exchange.	If an SSH session is started while another is in key-exchange phase, the first session will hang.	Made the key-exchange code re-entrant.
LAG members VLAN membership is confused.	Shutting down LAG member ports in a specific order can cause the first port shutdown to lose VLAN membership.	Update the VLAN membership masks correctly.
New stack manager can reboot while running IP Multicast traffic.	After failover, the new stack manager can reboot if IPv4 Multicast is running.	Failing to communicate with a stack member is no longer a fatal error.
VRRP does not recover from failover.	VRRP may not recover from the master failing.	Contention between flushing the ports and installing a new VMAC.
Contention adding and deleting multicast routes.	Switch could crash when using maximum number of multicast routes.	Corrected synchronization issue to keep driver and hardware in synch.
Crash while reloading unit with routing and spanning tree	Switch may crash when unit which contains one of the ports in a routing VLAN is reloaded.	Corrected return code when a stack message send fails.
DAI commands missing in port-channel mode	The dynamic ARP inspection commands are missing from port-channel interface configuration mode.	Added missing commands.

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

Description	User Impact	Resolution
Polycom 670 IP phones not receiving Voice VLAN	Phones which use CDP cannot connect to the Call Manager with the same configuration which worked on release 2.2.	Modified the policy rule to enable CDP frames flooding when ISDP is disabled so that call manager on the network side of the DUT responds with the Voice VLAN for the voip devices using CDP frames.
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 <b>snmp-server host &lt;ipaddress&gt;</b> and so may try to give IPV6 address as input.	Updated the help string to mention that IPv4 address is expected as input for <b>snmp-server host &lt;ipaddress&gt;</b> 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 <b>no</b> command to remove <b>switch x priority x</b> .	The <b>no switch 2 priority 2</b> command does not work. There is no <b>no</b> form for	Added the <b>no</b> 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 <b>show system id</b> 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	Configured non-existing host cannot be deleted for logging syslog.	Corrected logic so that only valid servers could be deleted.

Description	User Impact	Resolution
logging syslog.		
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'   " "   '@'   '#'   '\$'   '_'   '-'   '.'
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 <b>Last Frames Source</b> in the web page <b>EAP Statistics</b> .	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.

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

Description	User Impact	Resolution
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.
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.

Description	User Impact	Resolution
Adding VLAN range issues.	<ol style="list-style-type: none"> <li>1. When adding a range of VLANs to VLAN Database from Web Interface, an error message is returned when no name is entered.</li> <li>2. VLAN range is limited to 4 characters preventing adding certain ranges.</li> </ol>	<ol style="list-style-type: none"> <li>1. Corrected the error handling for this scenario.</li> <li>2. Increased the maximum length to 250 such that a comma separated VLAN list can be configured.</li> </ol>
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.
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 web page IP MTU 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 retrieve all of the applicable interfaces.

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

Description	User Impact	Resolution
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.
The switch will reset when Mitel phones are upgrading their firmware via the call manager.	The switch will reset and the phones will successfully upgrade. Once the switch reboots the phones operate properly.	Corrected switch software to not reference a memory location that has already been freed.
AutoConfig Install Fails after TFTP Bootfile loads to Stack	Using AutoConfig on a stack may result in the bootfileBrief.cfg contents not being updated properly on a stack member and the following message being displayed: <190> AUG 08 11:44:00 10.10.10.170-1 AUTO_INST[219139936]: auto_install_control.c(1619) 2500 %% AutoInstall<->CLI : File bootfileBrief.cfg is inconsistent	Ensure that the auto-install tmp file is properly deleted for all success and failure scenarios.

## Deprecated Commands and Parameters

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

Title	Description
<b>bridge address</b>	Interface Configuration mode  Rationale: The following parameters have been deprecated: <ul style="list-style-type: none"> <li>• <b>delete-on-reset</b></li> <li>• <b>delete-on-timeout</b></li> <li>• <b>secure</b></li> </ul>
<b>ip dhcp filtering</b>	Global Configuration mode  Rationale: The <b>ip dhcp filtering</b> command has been deprecated. It has been replaced by the <b>ip dhcp snooping</b> command.
<b>ip multicast staticroute</b>	Global Configuration mode  Rationale: The <b>ip multicast staticroute</b> command has been deprecated. It has been replaced by the <b>ip mroute</b> command.
<b>ip dhcp filtering trust</b>	Interface Configuration mode  Rationale: The <b>ip dhcp filtering trust</b> command has been deprecated. It has been replaced by the <b>ip dhcp snooping trust</b> command.
<b>show ip dhcp filtering</b>	Privileged EXEC mode  Rationale: The <b>show ip dhcp filtering</b> command has been deprecated. It has been replaced by the <b>show ip dhcp snooping</b> command.
<b>mdix</b>	Interface Configuration mode  Rationale: The <b>mdix { auto   on }</b> command has been deprecated. Crossover is always automatically detected on ports.
<b>port security</b>	Interface Configuration mode  Rationale: The following parameters have been deprecated:

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

Title	Description
	<ul style="list-style-type: none"> <li>• <b>forward</b></li> <li>• <b>discard-shutdown</b></li> </ul>
<b>logging buffered size</b>	<p>Global Configuration mode</p> <p>Rationale: The <b>logging buffered size</b> command has been deprecated. The buffer size is now fixed at 400 entries.</p>
<b>rmon table-size history</b>	<p>Global Configuration mode</p> <p>Rationale: The <b>rmon table-size history</b> command has been deprecated. The RMON history table size is now fixed at 270.</p>
<b>rmon table-size log</b>	<p>Global Configuration mode</p> <p>Rationale: The <b>rmon table-size log</b> command has been deprecated. The RMON log table size is now fixed at 100.</p>
<b>spanning-tree bpdu filtering</b>	<p>Global Configuration mode</p> <p>Rationale: The <b>spanning-tree bpdu filtering</b> command has been deprecated. It has been replaced by the <b>no spanning-tree bpdu flooding</b> command.</p>
<b>MSTP Mode</b>	<p>MST mode</p> <p>Rationale: The <b>abort</b> and <b>show</b> commands in MST Configuration mode have been deprecated.</p>

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

## CLI Reference Manual Updates

### iSCSI Configuration

Title	Description
<i>iscsi enable</i>	<p>Use this command to enable detection of EQL arrays via LLDP. Use the no form to disable detection of EQL arrays via LLDP.</p> <ul style="list-style-type: none"> <li>• Applies mtu 9216 on all ports and port-channels</li> <li>• Enables flow-control globally</li> <li>• Enables detection of EQL arrays via LLDP</li> </ul> <p><b>Default:</b> disabled.</p>
<i>no iscsi enable</i>	

### Non-Stop Forwarding

Title	Description
<i>nsf</i>  <i>no nsf</i>	<p>Use this command to enable non-stop forwarding. The “no” form of the command will disable NSF.</p> <p><b>Default:</b> Non-stop forwarding is enabled by default.</p>
<i>show nsf</i>	<p>Use this command to show the status of non-stop forwarding.</p> <p><b>Default:</b> Not applicable</p>
<i>show checkpoint statistics</i>	<p>Use this command to display the statistics for the check pointing process.</p> <p><b>Default:</b> Not applicable</p>
<i>clear checkpoint statistics</i>	<p>Use this command to clear the statistics of the check pointing process.</p> <p><b>Default:</b> Not applicable</p>
<i>vlan routing vlanid [index]</i>	<p>This command is used to enable routing on a VLAN. Us the “no” form of the command to disable routing on a VLAN.</p> <p><b>Default:</b> Routing is not enabled on any VLANs by default.</p>

Title	Description
<b><i>nsf [ ietf ] [ planned-only ]</i></b>	<p>Use this command to enable OSPF graceful restart. Use the “no” form of this command to disable graceful restart.</p> <ul style="list-style-type: none"> <li>• <b>ietf</b> — 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</li> <li>• <b>planned-only</b> — 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 <b>initiate failover</b> command).</li> </ul> <p><b>Default:</b> Graceful restart is disabled by default.</p>
<b><i>nsf helper [ planned-only ]</i></b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>planned-only</b> — This keyword indicates that OSPF should only help a restarting router performing a planned restart.</li> </ul> <p><b>Default:</b> OSPF may act as a helpful neighbor for both planned and unplanned restarts.</p>
<b><i>nsf [ietf] helper strict-lsa-checking</i></b>  <b><i>no nsf [ietf] helper strict-lsa-checking</i></b>	<p>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.</p> <p><b>Default:</b> A helpful neighbor exits helper mode upon a topology change.</p>
<b><i>nsf [ietf] restart-interval seconds</i></b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>ietf</b> — 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.</li> <li>• <b>seconds</b> — 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</li> </ul>

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

Title	Description
	seconds). <b>Default:</b> The default restart interval is 120 seconds.
<b><i>show ip ospf</i></b>	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.
<b><i>show ip ospf neighbor</i></b>	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: <ul style="list-style-type: none"> <li>• Helping – This router is acting as a helpful neighbor to this neighbor.</li> <li>• Not Helping – This router is not a helpful neighbor at this time.</li> </ul>

### Port Configuration Show Command

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

### Custom Protocol Based VLANs

Title	Description
<b><i>vlan protocol group add protocol &lt;groupid&gt; ethertype &lt;value&gt;</i></b>  <b><i>no vlan protocol group add protocol &lt;groupid&gt; ethertype &lt;value&gt;</i></b>	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. <ul style="list-style-type: none"> <li>• groupid—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the <b>vlan protocol group</b> command. To see the group ID associated with the name of a protocol group, use the <b>show port protocol all</b> command.</li> <li>• ethertype—The protocol you want to add. The ethertype can be any valid hexadecimal number in the range 1536 to 65535.</li> </ul>

	<b>Default:</b> Not applicable
<b>vlan protocol group</b> <groupid>  <b>no vlan protocol group</b> <groupid>	<p>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 <b>vlan protocol group</b> &lt;groupname&gt; is updated to <b>vlan protocol group</b> &lt;groupid&gt; so that groupid is used for both configuration and script generation.</p> <ul style="list-style-type: none"> <li>groupid—The protocol-based VLAN group ID, to create a protocol-based VLAN group. To see the created protocol groups, use the <b>show port protocol all</b> command.</li> </ul> <p><b>Default:</b> Not applicable</p>
<b>vlan protocol group name</b> <groupid> <groupName>  <b>no vlan protocol group name</b> <groupid>	<p>This is a new command for assigning a group name to vlan protocol group id.</p> <ul style="list-style-type: none"> <li>groupid—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the <b>vlan protocol group</b> command. To see the group ID associated with the name of a protocol group, use the <b>show port protocol all</b> command</li> <li>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.</li> </ul> <p><b>Default:</b> Not applicable</p>

#### VLAN Name Support with RADIUS Server

Title	Description
<b>show dot1x Ethernet</b> <i>interface</i>	<p>The command was updated to display the VLAN Id, or name as required.</p> <p><b>Default:</b> Not applicable</p>

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

## RADIUS Accounting Servers

Title	Description
<b>radius-server host acct</b>	<p>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.</p> <p><b>Default:</b> Not applicable</p>

## Spanning Tree

Title	Description
<b>no spanning-tree transmit hold-count</b>	<p>The hold-count keyword is not required when resetting the spanning-tree transmit hold-count.</p> <p><b>Default:</b> Not applicable</p>

## Stacking/CX-4 Module Configuration

Title	Description
<b>stack-port</b> <unit>/<port-type> <port-num> {ethernet   stack}	<p>This command is used to configure a port on a CX-4 or stacking plug-in modules as either an ethernet or stack port.</p> <p><b>Default:</b> 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.</p>

## Configurable Message of the Day Banner

Title	Description
<b>banner motd</b> <message>	<p>Controls (enables or disables) the display of message-of-the-day banners. 'banner motd' enables the banner, and allows configuration of message-</p>

<b>no banner motd</b>	<p>of-the-day banners. Use 'no banner motd' to delete the message, and disable the banner.</p> <p><b>Default:</b> Disabled by default.</p>
<b>banner motd acknowledge</b>  <b>no banner motd acknowledge</b>	<p>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.</p> <p><b>Default:</b> Disabled by default.</p>

## Dot1X

Title	Description
<b>dot1x timeout guest-vlan-period</b>	<p>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.</p> <p><b>Default:</b> The switch remains in the quiet state for 90 seconds.</p> <p>Refer to the <i>Dell™ PowerConnect™ 6200 Series Systems CLI Reference Guide</i> for details.</p>

## Link Dependency Commands

Title	Description
<b>link-dependency group [ action { up   down } ]</b>	<p>Use the action command to control the operational state of the group based on the dependent links state.</p> <ul style="list-style-type: none"> <li><b>up</b> — Causes the group members to change their operational state to be opposite that of the dependent link.</li> <li><b>down</b> — Causes the group members to change their operational state to follow that of the dependent link.</li> </ul>

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

	<b>Default:</b> Not applicable.
--	---------------------------------

### Multicast

Title	Description
<b>ip pimdm mode</b> <b>ip pimdm query-interval</b> <b>show ip pimdm interface</b>	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

### Release 3.2.0.10

Summary	User Impact	Workaround
Power inline legacy does not work after reboot.	CISCO IP phones that require legacy power will not work after a stack reboot if the phones are attached to a 2 or greater switch stack.	The master unit in the stack contains the correct legacy PoE configuration.

### Release 3.2.0.9

Summary	User Impact	Workaround
802.1Q trunks with GVRP enabled from PC62XX to Juniper EX4200/EX8200 experience Packet loss.	Data packets are lost on the trunk between the PC62XX and the Juniper EX4200. The lost packet rate is ~0.001%.	None.
When upgrading from version 2.2.0.3 to 3.2.0.9, on rare occasion, the "Failed to recover link status" message will be issued.	The Link for the reported port will be down but the link status LED will report up and a there will be no ingressing/egressing traffic.	Reloading the switch clears the problem.
After adding static IPv6 routes with CLI, viewing the configured routes with Web interface corrupts Running-Configuration.	The running-configuration is corrupted.	Use the CLI to view the IPv6 routes.
Combo ports 1/g45 - 1/g48 do not pass traffic when no negotiation is set	After ports 1/g45-1/g48 are configured with no negotiation set, when the switch is reloaded these port do not pass traffic.	For links requiring fixed speeds, use ports 1 - 44.
When configuring the "permit ip host" ACL rule for Dynamic ARP Inspection, console locks up.	The console locks up while configuring ACL for Dynamic ARP Inspection.	None.
When assigning sflow to an interface, the wrong interface gets	Sflow configuration on any member unit port is being applied on same port of manager unit.	None.

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

Summary	User Impact	Workaround
the attribute.	For example configuration for 2/g1 is applied on 1/g1 (assume unit 1 is manager and unit 2 is member).	
An invalid SNMP query can result with an invalid ipAdEntNetMask.	Secondary Netmask configuration is not displayed for an interface IP Address, and the Netmask of the primary IP Address is shown instead.	Use the CLI to display the secondary IP address.
When using TACACs to authenticate user access to switch management AND a Management ACL is applied, no user login attempt is performed.	TACACs server logs show no authentication attempt when user enters switch login credentials..	The user can log in with local switch credentials via SSH.
Occasionally there is a VLAN 1 routing configuration problem when the VLAN 1 is configured in 2.2.0.3 and reloads into 3.2.0.7.	The problem happens when there is only one active port in VLAN 1 and the mode of this port is switched to general/access with "switchport mode general" CLI command.	Perform a "shutdown/no shutdown" on the active physical port that VLAN 1 belongs to.
HTTPS fails if HTTP is disabled.	The HTTPS becomes inaccessible after switch reboot if HTTP is disabled and HTTPS is enabled.	Startup configuration should enable HTTP and HTTPS. Then CLI is used to disable HTTP after HTTPS is enabled.
MLD snooping with "bridge multicast forbidden forward-unregistered" is not working together.	With "bridge multicast forbidden forward-unregistered" enabled on the VLAN it is not possible to ping between the two client machines.	None.
Hostname is not updated in Running-Config when the name contains periods '.'	The pervious host name is still used	Don't use periods in the host name.
QoS statistics are not reported accurately in Web GUI	Some counters show no statistics.	The problem is only in the Web GUI. Use the CLI to retrieve the statistics.

### Release 3.2.0.7

Summary	User Impact	Workaround
---------	-------------	------------

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 <b>enable</b> 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 <i>large</i> 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 interval 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	If DHCP server is enabled, then the user	None.

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

Summary	User Impact	Workaround
data changed flag set after booting from saved config.	may be prompted to save configuration changes even though no configuration changes have been made.	
Bridge multicast address is shown as MAC Address format in <b>show running-config</b> 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.	<p>When port is changed to forbidden mode from access mode, the log message below is generated that reports the wrong port number.</p> <pre>&lt;187&gt; OCT 12 08:39:03 10.131.6.173-1 DOT1Q[104741168]: dot1q_api.c(525) 2475 %% Port(88)</pre> <p>This log message is correct when a port from the base unit is selected.</p>	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.

Summary	User Impact	Workaround
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.
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.	<p>This behavior is a limitation of implementing egress ACLs on an ingress classifier.</p> <p>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.</p>
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	<p>The Windows Vista® client could fail to authenticate properly when the option to cache user credentials is selected.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. In <b>Control Panel → Network Connections</b>, right-click on the desired <b>Local Area Connection</b> and select <b>Properties</b>.</li> <li>2. In the <b>Properties</b> window, select the <b>Authentication</b> tab.</li> <li>3. Deselect the checkbox for <b>Cache user information for subsequent connections to this network</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>

## LACP

Description	User Impact
LAGs Supported	<p>Number of LAGs supported:</p> <ul style="list-style-type: none"><li>• Up to 18 Dynamic LAGs</li><li>• 48 Static LAGs</li></ul> <p>Limitations (stack of 12)</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>

## VLAN

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

## Layer 3

### IP Map

Description	User Impact
<b>ip default gateway</b> and <b>ip default route</b> are for different types of interfaces. <b>ip default gateway</b> is for the management interface and <b>ip default route</b> 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 <b>mark cos</b> and <b>assign queue</b> attributes.	This behavior is a known limitation of the PowerConnect 6200 series switches.

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

### ICMP

Description	User Impact
IPv4 Fragmentation support	<p>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).</p> <p>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.</p>
ICMP Error message generation	<p>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.</p>
ICMPv6 Packet Too Big	<p>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.</p> <p>The PowerConnect 6200 Series switches do not have the capability to enforce IP MTU on VLAN Routing interfaces..</p>

### Multicast

Description	User Impact
Multicast VLC streams are not received on VLC client on complex network topology.	<p>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.</p>

## 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 <b>msgauth</b> command. To reset values to the default, delete the server and add it back.
<b>ip igmp snooping leave-time-out</b>	The leave-time-out in the CLI reference manual is improperly documented as 1 – 3174 and it actually is 1 – 25.

### 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.

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

### 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