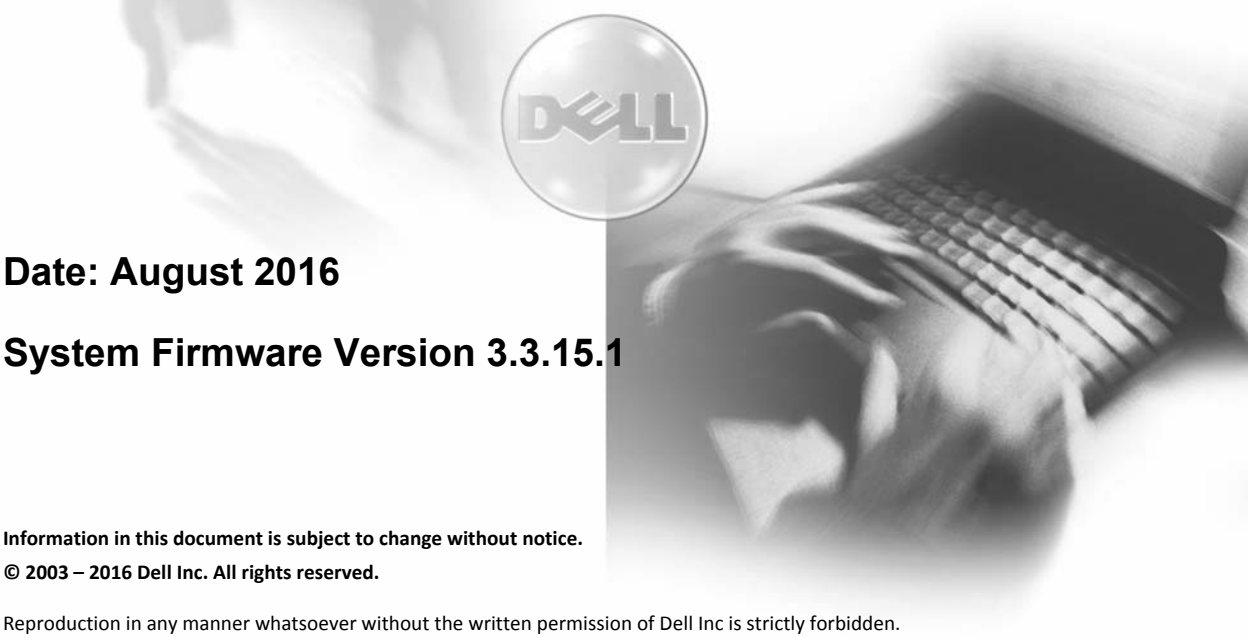
Dell™ PowerConnect™ 6224/6224F/6224P/6248/6248P

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

3.3.15.1 Firmware Release Notes



Date: August 2016

System Firmware Version 3.3.15.1

Table of Contents

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

Introduction

This document provides specific information for the Dell PowerConnect 6200 Series switches, firmware version 3.3.14.2.

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	3.3.15.1	Aug 2016

Firmware Upgrade

NOTE: Version 3.3.15.1 includes improvements to the firmware management system. You MUST follow the procedure set forth in the Dell PowerConnect 6200 Series Release 3.3.15.1 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 PC6224/6248 switches when stacked require that the same version of firmware be installed on every switch member.

Firmware Image Name	Version No.	Release Date
PC6200v3.3.15.1.stk	3.3.15.1	Aug 2016

Version Numbering Convention

	Version number				Description
PC6200	3	3	15	1	Four part version number
				↓	Denotes the build number.
			↓		Denotes an ad hoc release of the product software.
		↓			Denotes a scheduled maintenance release of the product software.
	↓				Denotes a major version number.

Supported Firmware Functionality

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

NOTE: If you use Open Manage 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 3.3.15.1 to a previous release is supported. Users should save their configuration file to a backup location before performing this operation. Migration of configuration information from a later release to an earlier release is not supported. It is strongly recommended that the current configuration be save locally (i.e., not on the switch) prior to downgrading the firmware. The existing configuration may or may not work with the earlier version of firmware, therefore, it is best to be physically present at the switch site and to be prepared to access the switch over the serial port if necessary when downgrading firmware.

Hardware Supported

PowerConnect 6224

PowerConnect 6248

PowerConnect 6224F

PowerConnect 6224P

PowerConnect 6248P

Added Functionality in this Release

Release 3.3.15.1

No new features introduced in Release 3.3.15.1.

Release 3.3.14.2

No new features introduced in Release 3.3.14.2.

Release 3.3.13.1

No new features introduced in Release 3.3.13.1.

Release 3.3.12.1

No new features introduced in Release 3.3.12.1.

Release 3.3.11.2

No new features introduced in Release 3.3.11.2.

Release 3.3.10.3

No new features introduced in Release 3.3.10.3.

Release 3.3.9.1

No new features introduced in Release 3.3.9.1.

Release 3.3.8.2

No new features introduced in Release 3.3.8.2.

Release 3.3.7.3

No new features introduced in Release 3.3.7.3.

Release 3.3.7.2

No new features introduced in Release 3.3.7.2.

Release 3.3.6.4

No new features introduced in Release 3.3.6.4.

Release 3.3.5.5

No new features introduced in Release 3.3.5.5.

Release 3.3.4.1

No new features introduced in Release 3.3.4.1.

Release 3.3.3.3

No new features introduced in Release 3.3.3.3.

Release 3.3.2.3

No new features introduced in Release 3.3.2.3.

Release 3.3.1.10

No new features introduced in Release 3.3.1.10.

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 themanagement unit fails, only the management switch needs to be restarted.

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

- Custom Protocol Based VLANs

  Prior to the 3.2 release only ARP, IP and IPX are configurable as protocols for protocol-based VLANs.

  This has been extended so that any Ethertype may be used.

- Port Configuration Show Command
  Added support for a single command that shows VLAN, STP, Port Status, and Port Configuration

  information etc.

  The new command is **show interfaces detail {ethernet** interface | **port-channel** port-channel-number} where

  - interface—A valid Ethernet port.
  - port-channel-number—A valid port-channel trunk index.

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

- VLAN Name Support with RADIUS Server

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

- HTTP Download

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

- Serviceability Tracing Commands

  Debug commands provided to enable tracing of various protocols.

- Faster Initialization for Stacking Failover

  Fast Reinitialization involves improvement in:

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

  Performance Improvements (based on Configuration File size) are:

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

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

- Auto Config

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

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

- DHCP Snooping

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

- DHCP L2 Relay

  Permits L3 Relay agent functionality in L2 switched networks.

- sFlow

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

- MLD Snooping (RFC2710)

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

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

- MGMD Proxy

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

- Dynamic ARP Inspection

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

- Multiple LLDP Neighbors per Interface

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

- Configurable DSCP for Voice VLAN

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

- CDP Interoperability

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

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

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

- SSH/SSL Refresh

  The SSH update incorporates the latest security and bug fixes.

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

- IPv6 support for QoS (ACL/DiffServ)

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

- Auto VoIP

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

- Dynamic ACL Management

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

- SCPv2, SFTP

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

- Captive Portal

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

users before access is granted.

- 802.1x MAC Authentication Bypass (MAB)

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

- Ping/Traceroute Enhancements

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

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

- Static Reject Routes

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

  This can be done for the following reasons:

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

- Clear ARP Cache Management Port

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

- OSPFv2 Point-to-Point Links

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

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

- OSPVv2/v3 Summary Reject Routes

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

- OSPF v2/v3 Passive Interfaces

  Allows passive interfaces for OSPF implementations.

- Granular OSPF v2/v3 Traps

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

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

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

- **network area** Command

  Support is added for the following 2 OSPFv2 CLI commands:

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

- OSPF v2/v3 Route Preferences Rework

  The following effects are seen with this change:

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

- Opaque LSAs and Detailed Display of OSPF v2 LSAs

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

by routers to distribute IP to link-layer address resolution information.

- ICMP Enhancements (RFC4443)

  ICMPv6 code is updated to support RFC 4443.

- DNSv6 Client

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

- Configured Tunnels MTU

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

- IPv6 6 to 4 Auto Tunnels

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

- VRRP Route Interface Tracking

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

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

- ICMP Throttling

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

  This project adds the following configuration options:
  - Rate limiting the generation of ICMP error messages.
  - Suppression of ICMP echo replies.
  - Suppression of ICMP Redirects.
  - Suppression of Destination Unreachables.

- IP Helper

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

- OSPF Enhancements

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

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

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

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

- IPv6 Management Enhancements

  Provides the following:

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

- Updated IPv4 Multicast Routing Support

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

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

- MLD Snooping Querier

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

Changed Functionality in this Release

Release 3.3.15.1

No changed functionality in Release 3.3.15.1

Release 3.3.14.2

No changed functionality in Release 3.3.14.2

Release 3.3.13.1

No changed functionality in Release 3.3.13.1

Release 3.3.12.1

No changed functionality in Release 3.3.12.1

Release 3.3.11.2

No changed functionality in Release 3.3.11.2

Release 3.3.10.3

No changed functionality in Release 3.3.10.3

Release 3.3.9.1

No changed functionality in Release 3.3.9.1

Release 3.3.8.2

No changed functionality in Release 3.3.8.2

Release 3.3.7.3

No changed functionality in Release 3.3.7.3

Release 3.3.7.2

No changed functionality in Release 3.3.7.2

Release 3.3.6.4

No changed functionality in Release 3.3.6.4

Release 3.3.5.5

No changed functionality in Release 3.3.5.5

Release 3.3.4.1

No changed functionality in Release 3.3.4.1

- Clarification of the ACL is as follows:

  There is an ACL HW table that can contain up to 24 VLANs. This is the ACL VLAN Id table. This table gets populated when an ACL gets applied to a VLAN. And, these are the VLANs that can have ACLs applied to them. There are 100 User ACLs that can be applied to interfaces like VLANs. And of these 100 ACLs, each ACL can be applied to any or all of the VLANs in the ACL VLAN table. So, the same ACL can be applied to many VLANS but these VLANs must be in the VLAN Id Tables. So, any of the 24 VLANs in the VLAN Id table can have up to 100 ACLs applied to them.

Release 3.3.3.3

- VoIP Phone Limits

  The limitation on the number of VoIP phones has been increased to 576 phones. Some VoIP phones use a location TLV and due to memory space on Kinnick are only able to support 128 location TLVs.

Release 3.3.2.3

No changed functionality in Release 3.3.2.3

Release 3.3.1.10

No changed functionality in Release 3.3.1.10

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

- **ip route** Command Changed

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

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

- **distance ospf** Command Changed

  The **distance ospf** command has been changed (for both OSPFv2 and OSPFv3) to the industry standard syntax. The new syntax is: **distance ospf** {**external** | **inter-area** | **intra-area** } *distance*

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

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

- **bridge address** Command Changed

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

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

- **secure**

- **port security** Command Changed

  The following port security command optional parameters have been deprecated:

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

- Link Dependency Available

  The Link Dependency feature which has previously only been available on modular switches is now available on all switches. The functionality is similar to the capability available on the PCM6220, PCM8024, and the PCM6348.
  This release added an action capability to link-dependency where if a dependant port goes down, as an action option, the group's members come up versus also go down. This can be used as a form of link redundancy as an alternative to using STP.

- ISDP Advertise/Display hostname

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

- Trap Configuration

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

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

- SNTP Server Priority

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

- GARP Leave Timer

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

- IP Multicast Static Route Configuration

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

- Support for Long User Names

  The **show users**, **show users accounts**, and **show users login-history** commands have changed. The **long**

parameter has been added to these commands to support long usernames.

- Flow Control

  Flow Control is enabled by default.

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

- VLAN Limit Increases

  MAC based VLAN limit was increased from 128 to 256.

  Subnet based VLAN limit was increased from 64 to 128.

- ACL Changes

  The following changes apply to ingress and egress ACLs:

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

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

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

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

- 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 3.3.15.1

Description	User Impact	Resolution
RADIUS Server Entry is Null or Could not allocate Radius Packet	The log message " RADIUS: Server Entry is Null or Could not allocate Radius Packet" is appearing even though the authentication was successful.	Corrected RADIUS database entry check.
Stack not passing traffic and cannot be accessed via console [PSE033282]	Crash in the SNMPTrapTask affects switch traffic.	Corrected data access problem by protecting the affected area by semaphore.

Release 3.3.14.2

Description	User Impact	Resolution
A VOIP component and floating point issue of SNTP causes the system to experience a software exception.	The system experiences a software exception when the system receives an invalid VLAN ID.	Corrected the VoIP and SNTP floating point error.
While evaluating the default gateway, the system displays the following message repeatedly: Failed to set the default gateway in the IP stack	While evaluating the default gateway, the system displays the following message repeatedly: Failed to set the default gateway in the IP stack	Corrected issue while evaluating default gateway.
Management access to the switch is lost due to the IP stack buffer leak.	Management access to the switch is lost due to the IP stack buffer leak.	Corrected an issue with IP stack buffer leak.
The "show interface counters" command does not display the output fully.	The "show interface counters" command does not display the output fully.	Corrected the output paging issue.
The DHCP snooping binding table has entries from VLANs that are not enabled for snooping.	The DHCP snooping binding table has entries from VLANs that are not enabled for snooping.	Corrected the check when snooping is enabled on a specific VLAN.

Description	User Impact	Resolution
The system displays bad target IP debug messages on the console.	Debugging messages are being sent to the console. The system displays bad target IP debug messages on the console.	The message is suppressed except when debugging is enabled.
"dot1sBpduReceive()" message is seen on the console.	The system displays the following message: "dot1sBpduReceive(): Discarding the BPDU, cannot get buffer from buff pool"	Corrected the issue that resulted in these messages.
The Dot1qTask process takes high CPU usage after applying a configuration to a port channel interface.	The Dot1qTask process takes high CPU usage when configuring the "voice vlan <vlanId>" command on an interface and the "switch port access vlan <vlanId>" command on a port-channel.	Corrected a looping issue when searching for VLANs.

Release 3.3.13.1

Description	User Impact	Resolution
Can't reach some IP when the destination IP is connected on unit1	Whenever reload is done on slave units, the trunk fails to synchronize with the newly added unit and an error message is thrown on the console.	Corrected issue in data retrieval when stack is reloaded.
Manually entered static arp entries not shown in 'show arp' output	Manually entered static arp entries not shown in the - show arp - output	Corrected manual ARP entry display issue.
OpenSSH Vulnerabilities	CVE-2006-4924, CVE-2006-4925, CVE-2012-0814, CVE-2010-5107, CVE-2014-1692, CVE-2014-2532.	Applied patches. The Nessus Scanner may still report the vulnerabilities based on the OpenSSH version number being used.
PCI DSS Compliance	Nessus 42873, 42800	Applied patches.
Stack crash	Radius receive task is not able to change the status of server entry from up to down when the respective routing interface goes down	Corrected Radius entry status issue.
ssltConnTask spiking up to 100 and causes switch to stop forwarding traffic	Continuously posted error SSI_ERROR_WANT_WRITE.	Corrected error closing SSL socket.
Stack reboots when OSPF adjacency changes occur.	OSPF NULL address causes switch to reload.	Corrected OSPF NULL address error.

Release 3.3.12.1

Description	User Impact	Resolution

Description	User Impact	Resolution
SSL/TLS MITM vulnerability (CVE-2014-0224)	OpenSSL SSL/TLS MITM vulnerability CVE-2014-0224	OpenSSL specified change for SSL/TLS MITM vulnerability CVE-2014-0224
dot1x command missing under interface range	The "dot1x timeout guest-vlan-period" is missing when trying to configure it under interface range	Added the interface range support for the command
POODLE vulnerability in SSLv3	The Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability allows a man-in-the-middle attacker to decrypt ciphertext.	Disabled SSLv3.

Release 3.3.11.2

Description	User Impact	Resolution
"ERROR: Boot code update failed" when attempt to update boot code on stack member	This message will apprear when requesting a boot code update before the stack initialization completes.	Corrected update boot code request issue.
Packet error counter increases when migrating from stacked to a LAG	Received packet discarded counter increases when pause frames are received.	Corrected counting of pause frames.
SSL Weak Cipher vulnerability (CVSS: 4.3)	SSL Weak Cipher vulnerability (CVSS: 4.3) Weak ciphers are available for use with SSL.	Weak ciphers are no longer available.

Release 3.3.10.3

Description	User Impact	Resolution
After initiate fail over connected ports are getting authenticated	After initiate failover occasionally there are some ports that are not configured for authentication but are being identified as authenticated.	Corrected authentication issue.
No link on SFP after upgrading from v2.2.x.	Occasionally upon upgrading from a 2.2.x version of firmware, Fiber ports may not link-up.	Corrected Auto-negotiation issue on fiber-ports.
SSH configuration not restored after reboot	SSH configuration 'ip ssh protocol 2' in the running config or startup config will be disregarded on next the boot.	Corrected configuration update issue.
10G stays down when unplugging/re-plugging cable	Occasionally, the 10G link on the plug-in module will not link-up if the cable is unplugged/re-plugged many times.	Corrected 10G phy initialization problem.

Description	User Impact	Resolution
Open SSH security vulnerability CVE-2010-5107	Open SSH telnet denial of service (connection-slot exhaustion) by periodically making many new TCP connections.	Applied OpenSSH patch for this issue. Note: many security scanners only check the version of the OpenSSH and report known issues based on that version. The version of OpenSSH did not change.
Open SSH security vulnerability CVE-2007-2243	Attempt to discover the existence of user accounts by attempting to authenticate via S/KEY.	Applied OpenSSH patch for this issue even though the firmware does not use this parameter. Note: many security scanners only check the version of the OpenSSH and report known issues based on that version. The version of OpenSSH did not change.

Release 3.3.9.1

Description	User Impact	Resolution
Error: osapiIfIpv6AddrsGet: could not get interface mottsec0! errno = 6	The following error has been reported: Error: osapiIfIpv6AddrsGet: could not get interface mottsec0! errno = 6	Corrected check for available service ports for IPv6.
Switch crash when using SSHv1	SSH session to the switch will result in a crash if SSHv1 with public key authentication is used.	Corrected memory leak in SSHv1.
OpenSSH security vunerability: CVE-2012-0814	OpenSSH security vunerability: CVE-2012-0814 will leak private information to ssh clients	Corrected information leak.
dot1x re-authentication problem on stacked switches	When a dot1x client is being re-authenticated it can occasionally fail if the client interface is through a stack unit.	Corrected dot1x client authentication on a stack unit.

Release 3.3.8.2

Description	User Impact	Resolution
Acceptable special characters in Interface description fields	CLI Command “description” will fail when startup-config is applied if the interface description field contains an apostrophe.	Corrected string parsing problem when encountering an apostrophe.

Description	User Impact	Resolution
Stack master crashes with atp_rx_thread error	Configuring a higher number of source ports in a mirroring session was causing the bcmATP-RX task to timeout.	Restricted the number of source ports that can be configured in a mirroring session to 8
Switch crashes if port unplugged during User radius login	The switch will crash when a Radius SSH client are on a "login:" prompt and are disconnected from the switch.	Corrected a buffer free problem when processing a Radius response.
Not possible to change logging level when server is configured	The command "logging <ip-address>" to enter into syslog command mode failed.	Corrected problem with the command "logging <ip-address>"
MS NLB cluster not reachable after rebooting the stack	NLB cluster not reachable after rebooting the stack due to trunk ID assigned to static MAC address.	Corrected trunk ID update problem.
SSH and Telnet not working	SSH and Telnet not working when failover to the standby unit of the stack.	Corrected problem when creating the new socket.
No Receive Discards counter available	Discards counter, ifInDiscards, is not available through the CLI.	Added "Transmit Packets Discarded" and "Receive Packets Discarded" to the "show statistics" CLI command.

Release 3.3.7.3

Description	User Impact	Resolution
Loss of switch management access with netPanic overflow messages after a few hours of switch uptime	Switch management is not accessible with the console errors: 0xca93d30 (ip6MapLocalDataTask): panic: jobQueueStdPost: out of QJOBs!	Corrected the problem by increasing the queue size (IPv6 packet buffer free) and addressed a logic problem to handle IPv6 multicast packets.

Release 3.3.7.2

Description	User Impact	Resolution
Telnet to port 80 hangs management.	Console occasionally hangs when telnet session to localhost is initiated.	Corrected telnet server port problem with loopback address.
SNMP dellVendorMIBObjects.hardware.productStatus not refreshing	SNMP Product Status OID value does not change after a fan/power failure and always shows 3.	Corrected a problem with checking the status of all the unit members in the stack
ISDP neighbor information is not consistent.	ISDP neighbor showed the other port's neighbor device ID.	Corrected a problem with gathering the neighbors interface information.

Description	User Impact	Resolution
Devices show up on incorrect ports in bridge table - dot1x mac bypass not working	Incorrect information is found in the bridge address table.	Corrected problem completely clearing the dot1x database on timeout.
Switch crashes with (ipMapForwardingTask): panic: jobQueueStdPost: out of QJOBS	Crash caused by memory buffer allocation failure.	Corrected problem returning memory buffer that was introduced in a previous fix.

Release 3.3.6.4

Description	User Impact	Resolution
Switch reboots when web server vulnerability test completes using Metasploit tool.	The exploit causes the switch to reboot, which takes several minutes, and can be used for a continual denial of service attack	Added a check for the length of the URL, if it exceeds 256 then set the length to 256, else use the URL length.
GVRP Interoperability issue with Dell Force10 S4810 switch	Dynamic bidirectional VLAN attribute registration is not working properly.	Corrected problem by implementing an action for the dynamic VLAN notification event.
Stops routing ipv6 traffic or responding to ipv4 management traffic	When running IPv6 traffic, IPv6 traffic eventually stops and IPv4 management traffic stops.	Corrected IPv6 problem.
File download via http fails	"File Download" option using 'http' produces "Error: File Transfer Failed".	Corrected HTTP download error.
File Upload ignores "Transfer File Path" in Web GUI	Unnecessary "Transfer File Path" field is shown on the "File Upload" page when transfer mode is HTTP.	Removed unnecessary "Transfer File Path" field on the "File Upload" page.
RFC2665/RFC3635 support (Pause Frames counters)	Pause frames counter cannot be obtained through SNMP.	Corrected SNMP problem in pause frame counters.
Incorrect Port Numbering - Output of "show power inline" CLI command	Port numbers are displayed incorrectly in the output of "show power inline" CLI command.	Corrected port numbering error.
Web user interface shows wrong switch image	The picture in the GUI represents a copper switch instead of fiber	Corrected port picture in the GUI.

Description	User Impact	Resolution
Unable to restore configuration file via http	"HTTP File Transfer is aborted. Management interfaces are released." message is logged to the console even if the script transfer succeeds.	Corrected error reporting transfer status.
Only able to view information for master unit in the stack via SNMP Walk.	Temp information can be retrieved for a stack master unit only, not for all members in the stack.	Corrected error in the retrieval of information from stack members.
SNMP Walk output for fan, power is not matching "show system" CLI output	SNMP and CLI output do not match for fan and power status of the switch.	Corrected SNMP data problem.

Release 3.3.5.5

Description	User Impact	Resolution
Error 404 when trying to upload configuration file through GUI using FQDN (Fully Qualified Domain Name).	If the hostname is used to login when attempting to upload a file using HTTP, the “page not found” error is thrown on the browser.	Corrected problem in resolving IP address.
Radius doesn't use specified source-IP address when address is from management	When the switch is used as L2 with IP address only on the management it will use this IP address as a source for a RADIUS authentication.	Corrected IP address check.
Switch cannot use the colon character in SNMP user-configured OID field	It is not possible to use colon character as part of the SNMP Location and Contact strings	Corrected the character-check to include the colon character.
Removing VLAN from general mode port affects VLAN routing	ARP packets are not forwarded to the CPU when a port is removed from one of the routing VLANs it participates in.	Corrected error in VLAN check.
Ping not working when the configuration is cleared and applied on the same VLAN	VLAN routing stops working once you remove and re-add the same VLAN.	Corrected error in the active VLAN check.
Non-Stop-Forwarding issue when using Port-channel spanned across stack members	Traffic lost during failover initiation for member port.	Corrected failover timing issue.
Switch crashes while sending LLDP stream	Switch crashes while sending LLDP stream.	Corrected error in the LLDP buffer pool.

Description	User Impact	Resolution
Log messages “l7utils_inet_addr.c(608) 135671 %% INET_ADDR:Invalid FamilyType – 0” logged during snmpwalk from OID .1	"Invalid FamilyType" log messages appear during snmpwalk from OID .1.	Corrected error when identifying Family Type.
Policy incorrectly gets applied in the GUI when ACL is also applied on the interface	Policy incorrectly gets applied in the GUI when ACL is also applied on the interface.	Corrected error in the ACL interface check.
Switch doesn't keep fixed speed LAG configuration after reboot	If LAG is configured to a fixed speed, after configuration is saved and then switch is reloaded, fixed speed configuration is lost and LAG will not be established.	Corrected error in saving LAG speed configuration.
Port detection mechanism fails with SNMP Query using Q-BRIDGE-MIB	dot1qVlanFdbId SNMP object returns incremental indexes of the VLANs	MIB was changed to return VLAN ids.
DHCP Request packets are not being forwarded to Voice VLAN Component	When using some VoIP phones, a phone on a switch running dot1x, the phone will not get authenticated and thus will not boot	Corrected error in dot1x forwarding

Release 3.3.4.1

Description	User Impact	Resolution
Switch displays unwanted logs	After applying a configuration script and clearing the configuration the switch displays unwanted logs.	Corrected the check that caused the unwanted logs.
Invalid Local7.Error.	An invalid Local7.Error error message is being produced.	Corrected the condition that caused the invalid error message.
Management ACL blocks TFTP traffic.	TFTP uploads or downloads are not allowed if any access-class is activated.	Corrected the condition that corrupted the TFTP information.
ISDP packets generating checksum errors on remote device	Checksum errors were being detected on the remote switches causing the packets to be dropped.	Corrected the ISDP checksum calculation for ISDP V2 packets.
Incomplete LLDP Med PDU discarded in some situations	Some LLDP MED PDUs are discarded on the switch because of incomplete TLVs.	Properly handled incomplete LLDP-MED TLVs.

Description	User Impact	Resolution
Unable to configure DVLAN / QINQ	Unable to configure ethertype globally.	Corrected the condition that caused DVLAN tagging to fail.
Stack instability in certain configurations	Stack will crash intermittently.	Corrected the stacking port memory leak.

Release 3.3.3.3

Description	User Impact	Resolution
VLAN trunk traffic issue when routing is removed from a VLAN	ARP packets are not forwarded to the CPU when LAG is a member of more than 1 routing VLAN and routing is disabled on one of them.	Corrected ARP forwarding policy when LAG is participating in the VLAN.
Performance degradation via default gateway after stack member restart	Upon reset default gateway does not get added back to the remote units.	Corrected the remote unit default gateway sync on restart.
When the stack Master is down the failover unit is unable to forward traffic	After failover the state of the port remains in blocked state.	Corrected port state after failover.
In RSTP, change in port cost results in no change of forwarding port	The changed value is not reflected in the show spanning-tree blockedport and show spanning-tree ethernet commands.	Corrected these commands.
IGMP snooping not functioning correctly	Occasionally, Multicast entries will not be learned if an IGMPv3 record comes in with TO_EXCLUDE mode.	Corrected TO_EXCLUDE mode processing.
IPMC error message in Kinnick platform	Error message indicates that the port is not part of the VLAN when setting the IPMC replication table	Corrected this condition.
Second link-dependent port does not bring down group members	Bringing down some ports will not bring down group members.	Corrected the group state when a port was brought down.
Control plane affected by L2 multicast	Multicast traffic affecting control plane management	Blocked L2 multicast from control plane
LLDP process crash with SNOM phones	LLDP process crashing with SNOM phones	SNOM phones not crashing LLDP

Release 3.3.2.3

Description	User Impact	Resolution

Description	User Impact	Resolution
Packets with TCP src/dest port 5060 not getting prioritized properly.	Protocol based Auto VOIP is not prioritizing SIP traffic over TCP port 5060 traffic	Corrected protocol qualifier problem with SIP traffic.
Management ACL service type option differs between CLI and Web.	Management ACL service type option is 'NONE' in WEB and is 'any' in CLI.	Corrected Web interface to match CLI.
Link Status is not displayed correctly	Link Status should be displayed as D-Disable instead of D-Down, when a BPDU Guard / protection enabled port receives BPDU.	Corrected error in the display of the status.
Port-channel interface has 2 stat counters.	Port-channel interface has 2 stat counters "1519-1522 octets" and "1519-2047 octets".	"1519-1522 octets" is incorrect and has been removed.
VRRP routing instances increased to 50.	VRRP routing instances increased to 50.	Increased VRRP routing instances table.
PC62xx with negotiation disabled and speed/duplex	With negotiation disabled and speed/duplex when a description is added to that port, the port reverts back to auto neg	Corrected an error when Auto-negotiation is disabled.
PoE for Cisco Wireless 1130AG	CDP/ISDP devices might not work in various ports with various sw builds.	Corrected error on ISDP packet checksum calculation.
PIM BSR join messages.	PIM Join messages using wrong RP Address	Corrected Join without a Prune condition.
When failing over stack master configuration is lost.	The configuration of other stack units is lost when the stack master fails over to the standby.	Corrected an error when initializing the newly formed stack after a failover.
Switch console locks, management not available if FTP is selected to copy config files.	Console locks up if we try to upload a file via FTP.	FTP is not supported. Use TFTP. Corrected an error check and provided an error message.
Telnet client has issues with setting terminal parameters	DNS and telnet log messages will appear when the session is initiated through telnet and outbound telnet is performed.	Corrected an error when resetting the internet address.
IP PIMSM BSR/RP Mapping is not robust	When the RP or the BSR changes, the data traffic may get affected and in some case get software forwarded.	Corrected RP join processing.
Change Error Message to "Specify interface for link-local destination"	Change Error Message to "Specify interface for link-local destination"	Changed error message.

Description	User Impact	Resolution
Change help string for destination in command "show sflow 1 destination"	Change help string for destination in command "show sflow 1 destination"	Changed help string.
In RSTP, change in port cost results in no change of forwarding port	When the cost of an interface is changed in STP/RSTP mode, the changed value is not reflected in the spanning tree commands.	Corrected error when calculating port costs.
PIM-SM Not all data passed down to the RPT.	When network re-configuration happens, the multicast trafffic may not properly converge thus resulting in loss of some traffic.	Corrected Join condition.
PIM-SM RP Fails to send Register Stops.	Register-Stop messages may not be sent out on the correct interface through to the First Hop Router.	Corrected Register Stops message error.
PIM-SM Joining messages using wrong RP address	PIM-SM Joining messages using wrong RP address	Corrected Join message processing.
Fails to reconfigure and forward multicast message	Switch fails to reconfigure and forward multicast messages following link failure	Correct an RPF information problem when link goes down.
PIM-DM Prune states expiring.	The router might end up sending Graft messages even though there are no intended hosts.	Corrected a PIM-DM timeout error.
Flow control negotiation issues with 10GBase-T module	Both switches report a different Flow control status for that link.	Updated the 10GBase-T PHY driver.
Discrepancy between GUI statistics and CLI statistics	show rmon statistics ethernet 1/gXX do not match what is display on the Web	TheReceived/Transmitted Rate (MFrame Bits/Sec) fields are not available from the WEB GUI.
PC6248 unable to set speed 1000 from CLI	Adding command for 1000mb forced speed	Added the "speed 1000" into CLI tree and let low layer decided whether it is supported or not?
PC6248 Port 25 fails to Link up	Port 25 unusable with 3.3.1.10	Corrected an error in port configuration
Switch crashes when using LLDP-MED	Switch crashes when using LLDP-MED	Corrected an error when adding LLDP TLVs.

Release 3.3.1.10

Description	User Impact	Resolution
Access is allowed to files on the switch without log in permissions required	If the file name is known, the file can be downloaded through the web browser without having to be logged in.	Corrected the web process to require login credentials before downloading a file.

Description	User Impact	Resolution
Stacked switches crash due to LLDP process	Stack crashes when LLDP TLVs are processed.	Corrected the release of memory when processing has completed.
Summertime function running early	The summertime function resets the time on the wrong week.	Corrected the function that returns the day of the week to account for particular months and leap years.
VLAN trunk traffic issue when routing is removed from a VLAN.	ARP packets are not forwarded to the CPU when a port is a member of more than 1 routing VLAN and routing is disabled on one of them.	Multiple VLAN membership is checked before changing the ARP policy.
SNTP server address fails when the domain-name starts with a numeric number.	If the DNS name starts with a numeric value, it is considered as invalid DNS name.	Allow for a numeric value to be the first character in the DNS name.
A small number of lost packets over GVRP trunks	Packets can be dropped resulting in a slow loss of traffic whenever a redundant VLAN is added.	The existence of the VLAN was checked for before it was added.
Unable to register more than 8 Mitel phones via LLDP-MED	Unable to register the full amount of LLDP-MED devices.	Increased the TLV buffers needed to accommodate the number of physical port.
Not Updating Root Path Cost	RSTP is not Updating Root Path Cost correctly.	Corrected the calculation that returns root path cost.
Incorrect End Of Line characters.	Switch's Telnet client sends only LineFeed instead of LineFeed + Carriage Return for EOL.	Updated End of Line characters to include Carriage return.
The MachineType is incorrect	Machine type is “Powerconnect 6200” should be “PowerConnect 62xx”	The machine type “Powerconnect 6200” was changed to “PowerConnect 62xx”.
Not able to communicate with the Aruba controller.	When the PowerConnect 62xx is the Root switch the Aruba controller discards the packets.	Packets were discarded because of an incorrect packet length. The packet length was changed to conform to the standard.
LLDP on Port Channel issue.	Some LLDP frames were not being authorized correctly.	Corrected the LLDP port authorization.
VOIP packets are being processed when VOIP is admin disabled	VOIP packets are being sent to the CPU for processing even though VOIP is admin disabled.	The VoIP task will not process any packets if VoIP is not administratively enabled.
MIB banner returns wrong value.	Using the OID to retrieve the banner returns the wrong value.	Corrected the buffer that is used to return the banner value.

Description	User Impact	Resolution
Thermal LED on the Web page does not reset to green.	Thermal LED, in device view of the Web page, continues to glow in RED after the device temp falls below thermal threshold.	Corrected threshold logic for thermal LED.
Switch loses power line legacy setting after reload.	After a stack reload older devices that require the power line legacy setting enabled will not work.	Correctly save the power line legacy configuration for a stack reload.
Banner configuration is lost with a new stack master.	When a new stack master is elected the banner is not available.	Propagated the banner to the other members of the stack.
Banner cannot be deleted using the WebUI	The banner cannot be deleted from WebUI and acknowledge enabled or disabled, does not get deleted and re-appears in Web UI even though "apply changes" is clicked.	The web page was fixed to allow user to remove banner message.
Large MOTD Banner does not show up in running-configuration.	When a large MTOD banner is entered it is not saved in the running-configuration.	The input of the MOTD was changes to allow large a large MOTD banner.
Sflow polling cannot be configured.	Sflow polling cannot be configured under interface ethernet on non-master switch interfaces.	Corrected the initialization of the unit number based on stacking configuration.
QoS statistics are not reported accurately in Web GUI	QOS stats files like OfferedPackets and Discarded packets are not accurately reported.	Corrected the Web interface to the QOS statistics.
Stack Failover issues on LAGs	The PHYs will link even though the switching chip is not ready to receive data. Data will be dropped.	Hold the PHYs in reset until the switching chip is initialized.
SNMP going unresponsive.	The switches will stop responding to SNMP requests.	A semaphore now used to properly control SNMP and CLI access to common configuration data structures.
Viewing/Adding IPv6 Routes from Web interface corrupts static routes.	Static routes become corrupted.	The next-hop address check is corrected when accessing the static routes.
Sflow interface command assigns sampling to the wrong interface.	Sflow configuration on any member unit port is being applied on same port of manager unit.	The unit number is correctly fetched from the current context.
MLD snooping is not working correctly.	MLD Snooping will not learn the Link local multicast groups.	The Link Local scope checking is being properly performed.

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.

Description	User Impact	Resolution
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.
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 properly 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 be established 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.
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.

Description	User Impact	Resolution
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.
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.
dtlIpv6NeighEntryDelete() : 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.

Description	User Impact	Resolution
syslog server is displaying hostname for IP address	User could not see the configured syslog host name.	The output of the **show syslog-servers** command now shows what was configured.
XFP trap messages on console are incorrect	Misleading log messages	The correct message is now displayed.
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.

Description	User Impact	Resolution
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.
DHCP Snooping's D-DISABLE is not working on LAGs	DHCP Snooping’s rate limiting is not disabling properly on LAGs.	Disabled the rate liming 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.

Description	User Impact	Resolution
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.
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.

Description	User Impact	Resolution
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 reliable connect to the network upon booting.	Ensure that source MAC address is used to uniquely indentify 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.
“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 **dos-control** 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.

Description	User Impact	Resolution
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.
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	User is not aware that the only IPv4 address is accepted by the command	Updated the help string to mention that IPv4 address is expected as

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

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

Description	User Impact	Resolution
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.
Adding VLAN range issues.	1. When adding a range of VLANs to VLAN Database from Web Interface, an error message is returned when no name is entered. 2. VLAN range is limited to 4 characters preventing adding certain ranges.	1. Corrected the error handling for this scenario. 2. Increased the maximum length to 250 such that a comma separated VLAN list can be configured.
Switch gives error message when entered upper case letter for interface value.	On the interface ethernet CLI command, switch gives error message when entering interface names in upper case letters.	String is converted to lower case before processing.

Description	User Impact	Resolution
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 weg page IP MTI field do allow the following values to be configured: 0 or 68-9198.
PCs or clients do not authenticate after reboot and logging back on (802.1x).	Windows Vista clients were not getting re-authenticated after the PC rebooted.	Modified the state machine to move to connecting state to trigger the sending of the EAP-REQ packet.
Web Display of Rapid Spanning Tree only displays first 10 interface ports	The Rapid Spanning Tree Table web page would only display the first 10, and potential incorrect interfaces.	Corrected the web page backend API to retireve all of the applicable interfaces.
Web Global Portfast applies Portfast on trunk switchports	Activating global portfast from the Web Interface applies portfast to trunk interfaces (Switching>Spanning_Tree>Global_Settings). When removing portfast globally via the CLI, it will not remove it from trunks.	While applying Portfast via the GUI, no check was present to know what the switchport access of a particular interface was hence the portfast was being applied even on trunk switchports.

Description	User Impact	Resolution
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
bridge address	Interface Configuration mode Rationale: The following parameters have been deprecated: • **delete-on-reset** • **delete-on-timeout** • **secure**
ip dhcp filtering	Global Configuration mode Rationale: The **ip dhcp filtering** command has been deprecated. It has been replaced by the **ip dhcp snooping** command.
ip multicast staticroute	Global Configuration mode Rationale: The **ip multicast staticroute** command has been deprecated. It has been replaced by the **ip mroute** command.
ip dhcp filtering trust	Interface Configuration mode Rationale: The **ip dhcp filtering trust** command has been deprecated. It has been replaced by the **ip dhcp snooping trust** command.
show ip dhcp filtering	Privileged EXEC mode Rationale: The **show ip dhcp filtering** command has been deprecated. It has been replaced by the **show ip dhcp snooping** command.
mdix	Interface Configuration mode Rationale: The **mdix { auto | on }** command has been deprecated. Crossover is always automatically detected on ports.
port security	Interface Configuration mode Rationale: The following parameters have been deprecated: • **forward** • **discard-shutdown**
logging buffered size	Global Configuration mode Rationale: The **logging buffered size** command has been deprecated.

Title	Description
	The buffer size is now fixed at 400 entries.
rmon table-size history	Global Configuration mode Rationale: The **rmon table-size history** command has been deprecated. The RMON history table size is now fixed at 270.
rmon table-size log	Global Configuration mode Rationale: The **rmon table-size log** command has been deprecated. The RMON log table size is now fixed at 100.
spanning-tree bpdu filtering	Global Configuration mode Rationale: The **spanning-tree bpdu filtering** command has been deprecated. It has been replaced by the **no spanning-tree bpdu flooding** command.
MSTP Mode	MST mode Rationale: The **abort** and **show** commands in MST Configuration mode have been deprecated.
ip ospf	Interface Configuration mode Rationale: The **ip ospf** command has been deprecated. This functionality has been replaced by the **ip ospf area** command.
ip ospf areaid	Interface Configuration mode Rationale: The **ip ospf areaid** command has been deprecated. This functionality has been replaced by the **ip ospf area** command.
ip dhcp filtering	Global Configuration mode Rationale: The **ip dhcp filtering** command has been deprecated.
ip dhcp filtering trust	Interface Configuration mode Rationale: The **ip dhcp filtering trust** command has been deprecated.
show ip dhcp filtering	Privileged EXEC mode Rationale: The **show ip dhcp filtering** command has been deprecated.

CLI Reference Manual Updates

Storm-control

Title	Description
Storm-control broadcast	The supported syntax is **Storm-control broadcast [level *rate*]** where ***rate*** is a parameter to **level** and defined to be: The storm-control threshold as percent of port speed. Percent of port speed is converted to PacketsPerSecond based on 512 byte average packet size and applied to HW. By default storm-control (unicast/multicast/broadcast) is disabled. If a level parameter is not used, the default rate is 5

Alternate Store and Forward (ASF)

Title	Description
Alternate Store and Forward (ASF)	The following paragraph appears in all UGs: Alternate Store and Forward (ASF) The Alternate Store and Forward (ASF) feature reduces latency for large packets. When ASF is enabled, the memory management unit (MMU) can forward a packet to the egress port before it has been entirely received on the Cell Buffer Pool (CBP) memory. AFS, which is also known as cut-through mode, is configurable through the command-line interface. For information about how to configure the AFS feature, see the CLI Reference Guide, which is located on the Dell Support website at www.support.dell.com/manuals. **Note the "AFS" should be "ASF".**

iSCSI Configuration

Title	Description
iscsi enable ***no iscsi enable***	Use this command to enable detection of EQL arrays via LLDP. Use the no form to disable detection of EQL arrays via LLDP. • Applies mtu 9216 on all ports and port-channels • Enables flow-control globally • Enables detection of EQL arrays via LLDP **Default:** disabled.

Non-Stop Forwarding

Title	Description
nsf ***no nsf***	Use this command to enable non-stop forwarding. The "no" form of the command will disable NSF. **Default:** Non-stop forwarding is enabled by default.
show nsf	Use this command to show the status of non-stop forwarding. **Default:** Not applicable
show checkpoint statistics	Use this command to display the statistics for the check pointing process. **Default:** Not applicable
clear checkpoint statistics	Use this command to clear the statistics of the check pointing process. **Default:** Not applicable
vlan routing vlanid [index]	This command is used to enable routing on a VLAN. Us the "no" form of the command to disable routing on a VLAN. **Default:** Routing is not enabled on any VLANs by default.
nsf [ietf] [planned-only]	Use this command to enable OSPF graceful restart. Use the "no" form of this command to disable graceful restart. • **ietf** — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional • **planned-only** — This keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the **initiate failover** command). **Default**: Graceful restart is disabled by default.
nsf helper [planned-only]	Use this command to allow OSPF to act as a helpful neighbor for a restarting router. Use the "no" form of this command to prevent OSPF from acting as a helpful neighbor. • **planned-only** — This keyword indicates that OSPF should only help a restarting router performing a planned restart. **Default:** OSPF may act as a helpful neighbor for both planned an unplanned restarts.
nsf [ietf] helper strict-lsa-checking **no nsf [ietf] helper strict-lsa-checking**	This command is used to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs. Use the "no" form of this command to allow OSPF to continue as a helpful neighbor in spite of topology changes. Default: A helpful neighbor exits helper mode upon a topology change.

Title	Description
nsf [ietf] restart-interval *seconds*	Use this command to configure the length of the grace period on the restarting router. Use the "no" form of this command to revert the grace period to its default. • **ietf** — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional. • *seconds* — The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The restarting router includes the restart interval in its grace LSAs (range 1 – 1800 seconds). **Default:** The default restart interval is 120 seconds.
show ip ospf	This command has been enhanced to lists the values of the configuration parameters described above and the status parameters defined in the RFC 4750 MIB.
show ip ospf neighbor	This command has been enhanced to list the per neighbor graceful restart status described in the RFC 4750 MIB. Possible values for Restart Helper Status are as follows: • Helping – This router is acting as a helpful neighbor to this neighbor. • Not Helping – This router is not a helpful neighbor at this time.

Port Configuration Show Command

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

Custom Protocol Based VLANs

Title	Description
vlan protocol group add protocol <groupid> **ethertype** <value> **no vlan protocol group add protocol <**groupid> **ethertype** <value>	Previously only ARP, IP and IPX are configurable as protocols for protocol-based VLANs. This has been extended so that any Ethertype may be used. • groupid—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command. • ethertype—The protocol you want to add. The ethertype can be any valid hexadecimal number in the range 1536 to 65535. **Default:** Not applicable

vlan protocol group <groupid> **no vlan protocol group <**groupid>	If the user creates multiple vlan protocol groups, deletes one of them, and then saves the configuration, the older implementation of this command resulted incorrectly applying the groupids on reload. Hence, the existing command **vlan protocol group <**groupname> is updated to **vlan protocol group** <groupid> so that groupid is used for both configuration and script generation. • groupid—The protocol-based VLAN group ID, to create a protocol-based VLAN group. To see the created protocol groups, use the **show port protocol all** command. **Default:** Not applicable
vlan protocol group name <groupid> <groupName> **no vlan protocol group name <**groupid>	This is a new command for assigning a group name to vlan protocol group id. • groupid—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command • groupName—The group name you want to add. The group name can be up to 16 characters length. It can be any valid alpha numeric characters. **Default:** Not applicable

VLAN Name Support with RADIUS Server

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

RADIUS Accounting Servers

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

Spanning Tree

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

Stacking/CX-4 Module Configuration

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

Configurable Message of the Day Banner

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

Dot1X

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

Link Dependency Commands

Title	Description
link-dependency group [action { **up** | **down** }]	Use the action command to control the operational state of the group based on the dependent links state. • **up** — Causes the group members to change their operational state to be opposite that of the dependent link.

	• **down** — Causes the group members to change their operational state to follow that of the dependent link. **Default:** Not applicable.

Multicast

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

Storm-control Broadcast

Title	Description
Storm-control Broadcast	The “storm-control broadcast” previously documented as: *storm-control broadcast [level | rate]* Is correctly documented as: *storm-control broadcast [level rate]* Where rate is a parameter to the Level option

User's Guide Updates

DVLAN-Tunnel

When dvlan-tunnel is enabled on an interface, it makes it an uplink (service provider) port. All other ports on the switch now behave like access (customer) ports. In order to get the switch back to the default state with DVLAN disabled, all the ports configured need to be un-configured for DVLAN tunneling (no mode dvlan-tunnel) and the ethertype of the switch needs to be reset to 802.1Q.

UPLINK PORT (Service Provider (SP) Port)

If a single tagged (SP tagged) or double tagged packet (SP tag as outer tag) ingresses on this port, lets it pass through unchanged to the respective access or uplink ports.

If an untagged or single tagged (802.1Q Tagged) packet arrives, tags it with the configured ethertype and the service provider VLAN ID taken from its PVID.

ACCESS PORT (Customer Port)

Always tags packets on ingress. On egress strips all (SP) tags belonging to service provider VLANS. Packets are tagged on ingress with the configured ethertype and the service provider ID taken from its PVID.

INGRESS LOGIC AND SUBSEQUENT EGRESS BEHAVIOR

Ingress logic for packet types ingressing an uplink (SP) port.

Ingress Packet	Uplink (Service Provider). Action taken on ingress.	Packet seen on egress at another Uplink port on the switch.	Packet seen on egress at another Access port on the switch.
Untagged	Add a SP Tag	Single Tagged	Untagged
802.1Q Tagged	Add a SP Tag	SP+802.1Q Tagged	802.1Q Tagged
SP Tagged	Do Nothing	SP Tagged	Untagged
SP+802.1Q Tagged	Do Nothing	SP+802.1Q Tagged	802.1Q Tagged

Ingress logic for packet types ingressing an access (Customer) port.

Ingress Packet	Access (Customer). Action taken on ingress.	Packet seen on egress at another Uplink port on the switch.	Packet seen on egress at another Access port on the switch.
Untagged	Add a SP Tag	SP Tagged	Untagged
802.1Q Tagged	Add a SP Tag	SP+802.1Q Tagged	802.1Q Tagged

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 3.3.10.3

Summary	User Impact	Workaround
When Fiber Combo ports are configured with no negotiation and fixed speed of 1000, then the fiber ports will not linkup. Clearing the switch configuration with **clear config** command doesn't resolve	Setting no auto negotiation on a 1G port is not recommended.	None.

Release 3.3.9.1

Summary	User Impact	Workaround
lintermittent VRRP routing issues since dot1x was enabled	Intermittent VRRP routing failure when dot1x authentication fails. This Is not a dot1x issue but a routing issue.	None.
After initiate fail over connected ports are getting authenticated	After initiate failover occasionally there are some ports that are not configured for authentication but are being identified as authenticated.	Fixed in 3.3.10.3 release.

Release 3.3.8.2

Summary	User Impact	Workaround
Error: osapiIfIpv6AddrsGet: could not get interface mottsec0! errno = 6	As per the log message the function osapiIfIpv6AddrsGet() is failing when trying to fetch the ipv6 addresses on a service port. On PC62XX switches the service port is not present.	Fixed in 3.3.9.1 release.
dot1x re-authentication issue	There is a re-authentication issue when using MAC-based dot1x authentication only on stacked switches.	Fixed in 3.3.9.1 release.
Auto-negotiation issue with the particular transceivers (Ciena XCVR-000G85-850nm or Nortel networks AA1419013 850 nm) installed at	Switch fiber port may not link up	**Workaround:** Disable auto-negotiation and manually setting speed to 1G using the existing CLI commands "no negotiation" and "speed" respectively for fiber ports from interface configuration mode. **Note:** It should be noted that when partners

Summary	User Impact	Workaround
the partner switch, and the link came up after auto-negotiation was disabled at PC62xx switch.		on either side are in different modes, the behavior cannot be guaranteed.

Release 3.3.4.1

Summary	User Impact	Workaround
Ping not working when the configuration is cleared and applied on the same VLAN	VLAN routing stops working once you remove and re-add the same VLAN.	Reload the switch after removing and then re-adding the same VLAN.
No display in Console regarding to snmp-server traps except Authentication trap	Expecting the display of all configured traps when using the show SNMP command.	None.

Release 3.3.1.10

Summary	User Impact	Workaround
Web File Download	When downloading a file by means of the web interface, the file can remain in the browser cache.	Clear the browser cache when the file download has completed.

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”	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.

Summary	User Impact	Workaround
message will be issued.		
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 the attribute.	Sflow configuration on any member unit port is being applied on same port of manager unit. For example configuration for 2/g1 is applied on 1/g1 (assume unit 1 is manager and unit 2 is member).	None.
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	The HTTPS becomes inaccessible after switch reboot if HTTP is disabled and	Startup configuration should enable HTTP and HTTPS. Then CLI is used to disable

Summary	User Impact	Workaround
is disabled.	HTTPS is enabled.	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
Non-configuration file getting loaded to startup-config through HTTP.	When the switch reboots and attempts to read an invalid start-up configuration file, it will give up and create a default startup configuration.	It is recommended that all users keep backups of their configuration files.
TACACS operation	User cannot enter Privileged EXEC mode without using the **enable** command.	None.
Ping fails with 33% to 100% packet loss	Using a Windows 7 client and pinging with a 59900 byte packet will result in packet loss.	None.
OSPF Dead interval expires on neighbor, when the DUT stack manager restarts with *large* configuration.	In a large stack with an unusually large configuration, it is possible that during an unplanned failover, the control plane may not issue OSPF grace LSAs before the dead interval expires on neighbors. When this happens, neighbors report the router down and other routers in the area recomputed OSPF routes to avoid the restarting order.	Increase the dead internal timer.
VLAN configuration is not successful on ports after detaching them from LAG.	The issue is that any VLAN configuration applied to a physical port while it is a member of a LAG will not be applied when the port leaves the LAG.	This is not a problem if VLAN configuration is performed while the port is not a member of a LAG. If the configuration is saved and the switch is reset, the configuration is applied correctly.
Issue with PBVLAN configuration migration.	The command vlan protocol group expected a string in earlier versions; now it expects a number.	The software recognizes if the group name is alphanumeric, however it will not work when the name of the group is numeric (for example 2, 3, etc.)
R/W user is getting read only access when authentication	The user always gets Read-Only access if using TACACS as a means for HTTP authentication, even if the TACACS user is	User can configure the same TACACS user locally and use LOCAL authentication method for HTTP. The user will be able to

Summary	User Impact	Workaround
method is used as TACACS.	Read/Write capable.	get access based on this local user access level (Read-write or Read-only).
TFTP gives no reason for file download failures.	Generic failure message.	None.
CLI command stack-port config rejection does not display the cause.	If a user enters an invalid interface, a generic error message will be generated: ERROR: Invalid input.	None.
Banner MOTD: The switches Console and Web sessions are inaccessible until the user acknowledges the banner of the day.	The current implementation of the MOTD acknowledgement results in all user interface sessions being inaccessible until the user enters a response or the 30-second timeout occurs. While the acknowledge process is pending, it cannot process the other UI sessions. Once the timeout occurs, then the MOTD acknowledgement ends the connection and resumes processing of the other sessions.	Acknowledge the message to avoid the session timeout.
DHCP server has data changed flag set after booting from saved config.	If DHCP server is enabled, then the user may be prompted to save configuration changes even though no configuration changes have been made.	None.
Bridge multicast address is shown as MAC Address format in **show running-config** buffer when it is configured in IP format.	If a user configures the bridge multicast address as an IP address format in VLAN interface mode, it is displayed in the show running-config command in MAC address format.	None.
Connected spanning tree root port role not changed to auto-portfast after disabling MSTP on Trunk.	A port that is a root port will not become auto edge port if the bridge that the root port is connected to goes away.	This means that the port would flush the Forwarding Database entries every time that there is a topology change. This could be avoided if the link goes down and comes back up.
Three commands are not available at interface range Ethernet level, but are available at interface.	The following commands are not available to use in interface range Ethernet level: isdp, lacpa, and protocol.	Each interface must be configured individually.
There is no command to add protocol vlan in interface range mode.	The user cannot use interface ranges to configure a protocol VLAN.	Each protocol VLAN must be configured individually.

Summary	User Impact	Workaround
Invalid error port number displayed on log message when VLAN is changed to forbidden mode from access mode.	When port is changed to forbidden mode from access mode, the log message below is generated that reports the wrong port number. <187> OCT 12 08:39:03 10.131.6.173-1 DOT1Q[104741168]: dot1q_api.c(525) 2475 %% Port(88) This log message is correct when a port from the base unit is selected.	None.
Gratuitous ARP packets are not being generated when management VLAN is changed with static IP configuration.	If the user changes the management VLAN, then management connections must be re-established on the new VLAN. Neighbors will resolve the switch's management IP address on the new VLAN.	None.
Using interface range mode not able to configure protected ports.	Cannot use interface range mode to configure protected switchports.	The user must configure each protected port individually.
TFTP fails to display specific error message when incorrect filename was given while downloading the code.	If a user attempts to tftp a non-existent file to the image of the switch, nothing will be downloaded and there will not be an error message generated.	None.
Web needs to provide an option to configure sFlow sampler / poller values on range of interfaces.	User will not be able to select range of interfaces through web for the Sampler and Poll Configuration web pages. However, configuration is not affected as user can individually select the interfaces and configure.	User has to select each interface individually to configure in the Sampler Configuration and Poll Configuration web pages.
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.

Summary	User Impact	Workaround
When Line or enable method is used as login method and enable authentication is none, the user is unable to enter into Privileged EXEC mode.	If login authentication method is Line or Enable, and enable authentication is None, you will always get read-only access (because there is no user configured for line or enable authentication). The user will never get read-write access.	If enable authorization is set to None, ensure that the login authorization method is at least TACACS, Radius, or Local. Any authentication method that requires a user configuration will ensure that the user will get proper access based on how the user is configured.
Cannot change LAG mode from Static to Dynamic via CLI.	Cannot change LAG mode from Static to Dynamic via CLI.	The user may change the LACP Mode using the Graphical User Interface.

Known Restrictions and Limitations

Layer 2

802.1AB (LLDP)

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

QoS

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

802.1X

Description	User Impact
Windows Vista® Authentication	The Windows Vista® client could fail to authenticate properly when the option to cache user credentials is selected. Workaround: 1. In **Control Panel** → **Network Connections**, right-click on the desired **Local Area Connection** and select **Properties**. 2. In the **Properties** window, select the **Authentication** tab. 3. Deselect the checkbox for **Cache user information for subsequent connections to this network**. 4. Click **OK**.

LACP

Description	User Impact
LAGs Supported	Number of LAGs supported: • Up to 18 Dynamic LAGs • 96 Static LAGs Limitations (stack of 12) • Long Timeouts With a minimal CPU load, it takes approximately 1.5 minutes with 16 dynamic LAGs and 15 MSTP instances for the ports to become active with traffic running. • Short Timeouts With a minimal CPU load, it takes approximately 1.5 minutes with 12 dynamic LAGs and 15 MSTP instances for the ports to become active with traffic running.

VLAN

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

Layer 3

IP Map

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

DiffServ

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

ICMP

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

Auto VOIP

Description	User Impact
Auto VOIP sessions.	There is a limitation of 16 Auto VOIP sessions.

Multicast

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

Management

CLI

Description	User Impact
radius-server mode commands do not have a "no" form.	None of the commands in radius-server mode support a "no" form except for the **msgauth** command. To reset values to the default, delete the server and add it back.
ip igmp snooping leave-time-out	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.

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