Dell™ PowerConnect™ 5324

PowerConnect 5324 Release Notes

Date: August 2004
System Firmware Version 1.0.0.45

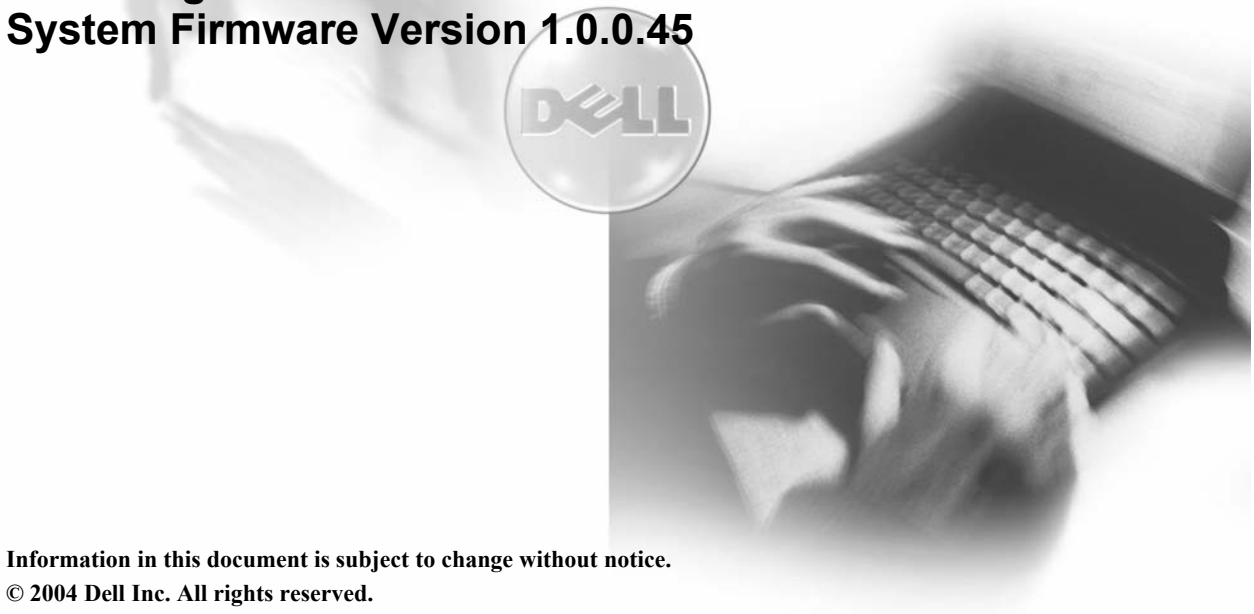


Table of Contents

PowerConnect 5324 Release Notes

Introduction

This document provides specific information for the Dell PowerConnect 5324 Switch system, firmware version 1.0.0.45.

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

GLOBAL SUPPORT

By Web: http://support.dell.com/

For information regarding the latest available firmware, recent release notes revisions, or if requiring additional assistance, please visit the http://www.dell.com Support Web Site.

Firmware Specifications

Firmware Version Details

Boot PROM Name	Version No.	Release Date
5324_boot-10020.rfb	1.0.0.20	August, 2004

Firmware Image Name	Version No.	Release Date
5324-10045.dos	1.0.0.45	August, 2004

The firmware image version should be 1.0.0.45 on the PowerConnect 5324. The boot prom image should be 1.0.0.20 Refer to the PowerConnect 5324 Getting Started Guide for instructions on loading the boot PROM software and updating the firmware image.

Version Numbering Convention

Version number					Description
5324	1	0	0	45	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 PowerConnect 5324 User Guide.

Added functionality in this release

Version 1.0.0.45 is the first software release of the PowerConnect 5324.

Issues resolved

Version 1.0.0.45 is the first software release of the PowerConnect 5324.

Known Restrictions and Limitations

Management

Web-based Management

Title	Description	ID
Presenting a full ARP table in Web-based management.	Presenting a full ARP table may take several minutes if the ARP table has a significant number of entries. **Workaround:** Use CLI to show full ARP table.	24828
Deleting an ACE using web interface	When deleting an ACE from an ACL using the web interface, the page refresh may take several minutes.	24835
Repeated authentication (Username/password) in navigation tree	Repeated authentication of Username and password window may be presented while using the navigation tree on the right hand side of the embedded web management. This system exhibits itself when the embedded web management is in the middle of presenting a requested management page and is interrupted by the user's clicking on a different page.	24400
Port configuration management using Mozilla Browser in Linux OS	When managing the device using Mozilla Browser in Linux OS and changing Flow Control (System->Switch->Ports->Port Configuration->Show All) from "Disable" to "Enable" and vice versa in one of the dropdowns, all other dropdowns under it change their values too.	25085

Telnet

Title	Description	ID
Telnet session fatal error message	When connected to a PowerConnect 5324 and the user connects to another switch ("second switch") using the "Telnet" command, a fatal error message will be displayed after 1) the second switch's telnet exec timeout period transpires and 2) the user resumes the operation of the terminated telnet session.	25837
Telnet launch from Unix/Linux web-browser	When a web-based browser running on Unix/Linux, clicking the Telnet button in the web-based management does not open a Telnet session.	25001

Security

SSH

Title	Description	ID
Serial connection is lost after 4 concurrent SSH sessions	An attempt to open a forth SSH session will cause the serial connection to the device to become inactive. **Workaround:** Do not open more than three concurrent SSH sessions.	24773
Deleting SSH generated crypto key	Once a key is generated (RSA or DSA), a key cannot be removed. **Workaround:** Erase the flash image and reload.	25047

802.1x

Title	Description	ID
802.1x authentication does not work when EAP packets are transmitted with a VLAN tag = 0	When 802.1x packets are transmitted with VLAN tag = 0, port cannot authenticate. **Workaround:** Do not use VLAN 0 for network configurations. Switch default VLAN is 1.	23215
Incorrect information displayed in "Authenticated Users" Web-based management page	Incorrect information displayed in "Authenticated Users" Web-based management page with no relevancy to 802.1x status (enabled or disabled) **Workaround:** Use CLI for “Authenticated Users” status.	25857

Configuration

Ping

Title	Description	ID
Ping packets sent from a network using a 10Mbps hub are lost	Ping packets that are sent from network using a 10Mbps hub are lost.	23043

Flow Control

Note: When FlowControl is disabled per interface, flow control will be disabled per device not per Interface.

Documentation updates

Introduction

This document lists the changes from the PowerConnect 5324 User's Guide. The modifications are due to instances discovered in various user environments.

General

The following must be changed globally:

Starting and Configuring the Device

Assigning Static IP Addresses on an Inband Interface

Modify the following:

Current	New
Console (config-if) # ip address 192.168.1.123/24 255.255.255.0	Console (config-if) # ip address 192.168.1.123 255.255.255.0

Configuring an Initial HTTPS Password

Delete the following:

Enter the following commands once when configuring to use a terminal, a Telnet, or an SSH session in order to use an HTTPS session.

Note: In the Web browser enable SSL 2.0 or greater for the page content to be displayed.

```
console(config)# crypto certificate generate key_generate
console(config)# ip https server
```

▪ Telnet Connection

To start communications using automatic baud detection, press the Enter key twice. The factory default is autobaud enabled and no synchronization between a terminal and a device is required during the initial device installation. If, during the operation, the terminal was replaced by another one or the speed mode was switched over on the device, the following must be taken into consideration:

- A blank screen appearing after reset is an indication that the terminal and the device are not synchronized. To activate the autobaud option, press the Enter key twice.
- If the autobaud option is enabled on the device, it automatically becomes operational after reset ONLY ONCE, after pressing the Enter key twice.

▪ Configuring Domain Name Systems

Under the Add DNS page add the following field description:

DNS Server — DNS Server Name. The name cannot start with a numeric character.

- **Defining a New Community**

Add extra instructions.

Current	New
5 Click Apply Changes. The new community is saved, and the device is updated.	5 Click Apply Changes. 6 Close Add SNMP Community page. The SNMP Community page is displayed. 7 Click Refresh. The new community is inserted.

Defining SNMP Traps

Add extra instructions.

Current	New
5 Click Apply Changes. SNMP traps are enabled on the card.	5 Click Apply Changes. 6 Click Refresh. SNMP traps are enabled on the card.

LAG Configuration

Defining LAG Parameters

Add to the description:

The LACP port channel can accept up to 16 ports but only 8 will be active at the same time.

Storm Control

Add to description: Storm Control is enabled per Gigabit ports by defining the packet type and the rate the packets are transmitted. Ports can also be grouped to provide Storm protection for the entire group.

Modify the CLI Command

Current	New
port storm-control broadcast enable	port storm-control broadcast enable [ethernet interface]

Modify

Field	Current	New
	Broadcast Rate Threshold (1-1000000)— The maximum rate (packets per second) at which unknown packets are forwarded. The range is 0-1000000. The default value is zero. All values are rounded to the nearest 64Kbps. If the field value is under 64Kbps, the value is rounded up to 64Kbps, with the exception of the value zero.	Broadcast Rate Threshold (0-65535) — The maximum rate (packets per second) at which unknown packets are forwarded. The range is 0-65535. The default value is zero. All values are rounded to the nearest 64Kbps. If the field value is under 64Kbps, the value is rounded up to 64Kbps, with the exception of the value zero. Note that if the rate is 0, broadcast packets are not forwarded.

Port Mirroring

Defining Port Mirroring Sessions

Add the following restriction:

A maximum of 8 ports can be monitored (both Rx and Tx).

Protocol Port

Modify the field name from **VLAN ID (1-4095)** to **VLAN ID** and add to the description (Range: 1-4094).

Configuring GVRP

Delete: To ensure the correct operation of the GVRP protocol, it is advised to set the maximum number of GVRP VLANs equal to a value which significantly exceeds the sum of:

- The number of all static VLANs both currently configured and expected to be configured.
- The number of all dynamic VLANs participating in GVRP, both currently configured (initial number of dynamic GVRP VLANs is 128) and expected to be configured.

RMON History Control

After the field **Max No. of Samples to Keep (1-65535)** add the following note:

Note: A change to the number of sample is only effective after a reboot.

Viewing Tables

Current	New
The Utilization Summary page contains statistics for interface utilization.	The Utilization Summary page contains statistics for **viewing** interface utilization.

- **GVRP Statistics**

Field	Current	New
Leave All	Device GVRP Leave all statistics.	Device GVRP Leave All statistics.

QoS

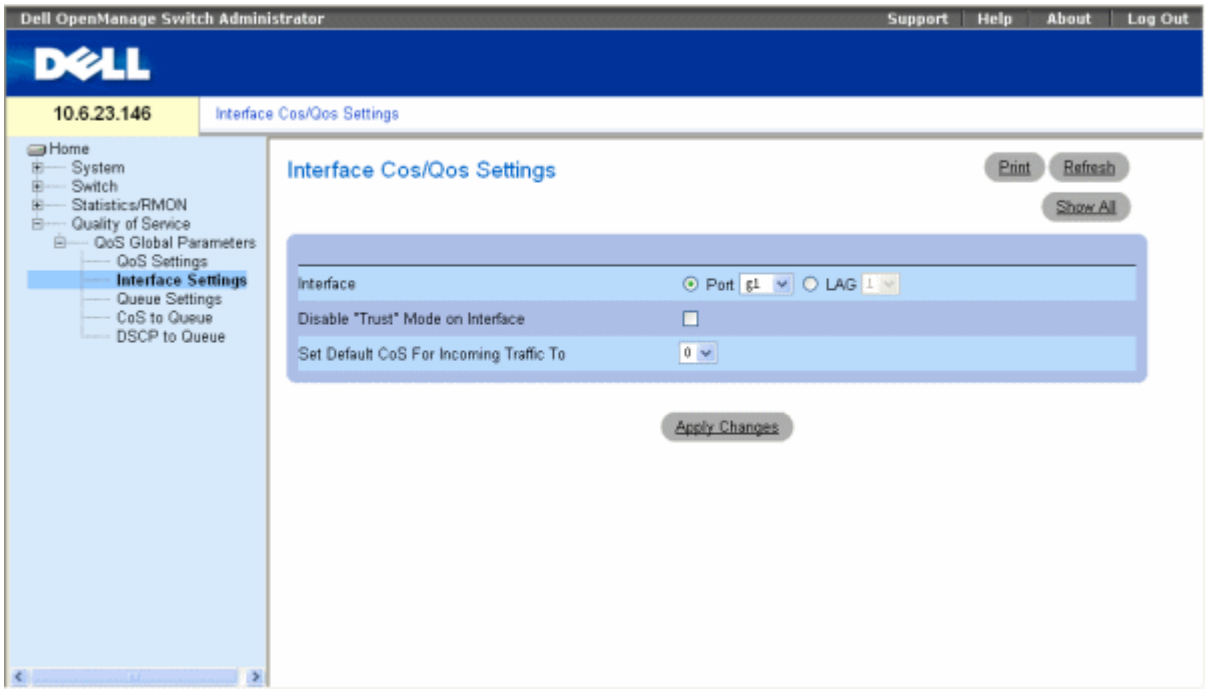
QoS Overview

Under the WRR description, change the following:

Current	New
The strict priority queue is emptied before the traffic in the remaining queues in forwarded.	The strict priority (SP) has priority over WRR, and where the traffic is low, WRR shares the bandwidth with SP, occupying the remaining bandwidth according to the calculated ratio.

Interface CoS/QoS Settings

The following Screens has been updated under the QOS section



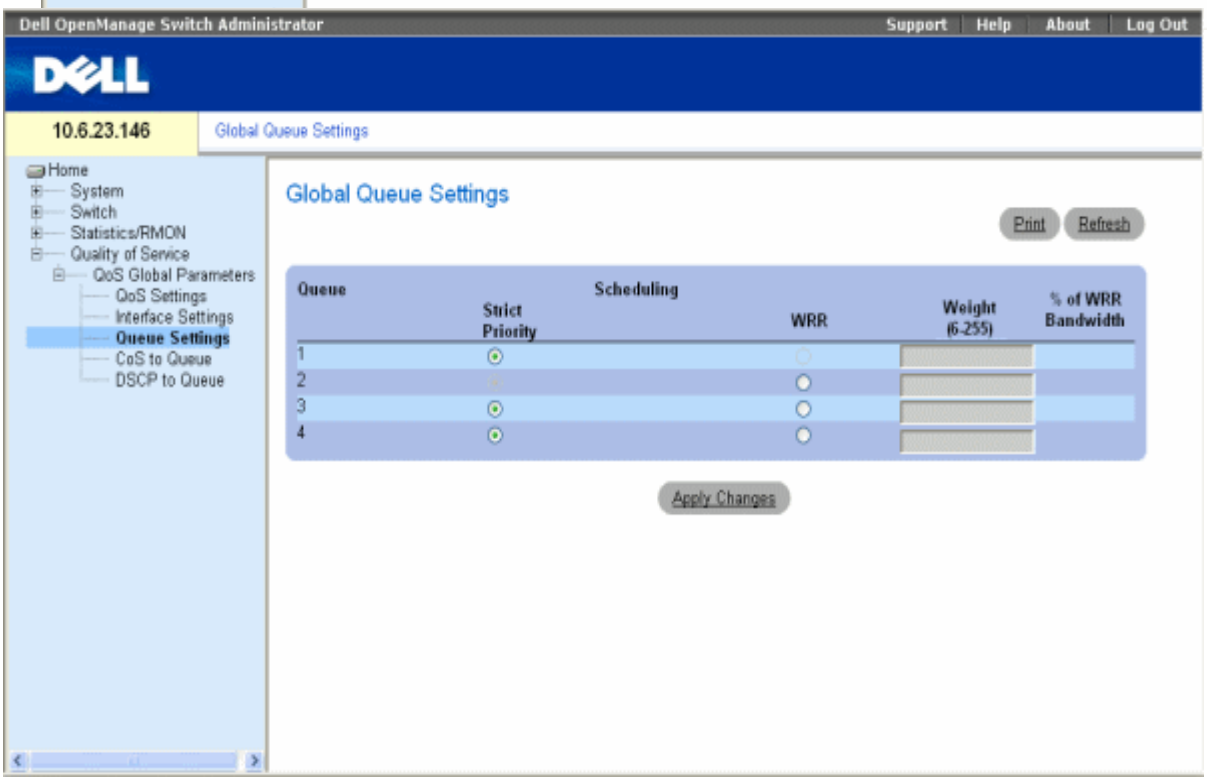
Remove the following field descriptions.

- **Queue** — The queue number.
- **Queue Mode** — Indicates whether the queue is Strict Priority or WRR. This is defined in the **Queue Settings** screen.
  - → SP can be configured on all queues 1 - 4. This is the default configuration.
  - → WRR can be configured on all queues 1 - 4.
  - → Two queues on WRR and two queues on SP. The options are as follows: SP mode can be configured on queues 1 - 2 and WRR on queues 3 - 4
  - → WRR mode can be configured on queues 1 - 2 and SP on queues 3 - 4
  - → WRR mode can be configured on queues 1 - 3, with SP on queues 4
- **Weight (0-255) —** Assigns WRR weights to queues. This field is enabled only for queues in WRR queue mode.
- **% of WRR Bandwidth** — The percentage translation of the weight defined in the **Weight (0-255)** field.

After the instructions for Assigning QoS/CoS settings for an interface, add the following instructions:

Displaying QoS/CoS settings:

1. Open the Qos/Cos page.
2. Click Show All.
   The Interface Table is displayed.



Add the following field descriptions below the current descriptions:

- **WRR —** Specifies if traffic scheduling is based on the Weighted Round Robin (WRR) weights to egress queues.
- **WRR Weight —** Assigns WRR weights to queues. This field is enabled only for queues in WRR queue mode. Each queue has a weight range, queues 1-3 have the range 0-255, and queue 4 has the range 1-255.

NOTE: If a queue is set to 0 weight, the queue is not operational and is effectively closed.

- **% of WRR Bandwidth** — The percentage translation of the weight defined in the **WRR Weight** field.

There are four optional Strict Priority (SP) to WRR configuration combinations:

- The default - 4 SPs
- 4 WRRs
- 2 WRRs + 2 SPs (1WRR, 2 WRR, 3 SP, 4 SP or 3 WRR, 4 WRR, 1 SP, 2 SP)
- 3 WRRs (1, 2 , 3) + 4 SP

Rapid Spanning Tree

Modify

Field	Current	New
Point-to-Point Admin Status	Enables or disables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link. To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs.	Enables or disables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link. To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual device port link type.
Point-to-Point Operational Status	The Point-to-Point operating state. This is the actual device port link type.	The Point-to-Point operating state. It may differ from the administrative state.

Network Security

Under the heading Network Security" enter the following note:

If navigating between the Network Security pages, wait for the page to load completely before navigating to another page. If not, some instances display a password prompt, as the previous page has not completed dealing with the user information before being closed. The system views the new screen as a new user.

Multiple Hosts

Modify

Field	Current	New
Action on Single Host Violation	Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address. The **Action on Single Host Violation** field can be defined only if the **Multiple Hosts** field is defined as **Disable**. The possible field values are: ♦ **Permit**— Forwards the packets from an unknown source, however, the MAC address is not learned. ♦ **Deny** — Discards the packets from any	Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address. The possible field values are: ♦ **Forward** — Forwards the packets from an unknown source, however, the MAC address is not learned. ♦ **Discard** — Discards the packets from any unlearned source. This is the default value.

	unlearned source. This is the default value. ♦ **Shutdown** — Discards the packet from any unlearned source and locks the port. Ports remain locked until they are activated, or the device is reset.	♦ **Discard Shutdown** — Discards the packet from any unlearned source and locks the port. Ports remain locked until they are activated, or the device is reset.

Port Security

In the introduction, under the “Unauthorized packets arriving to a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- The ingress port is disabled”

Note: In order to enable port security, the Multiple Hosts feature must first be enabled on the required port(s).

Port Configuration

Before the CLI example, enter the following Note:

Note: When device wakes up with autobaud enabled, press "Enter" twice to activate the autobaud.

Radius Settings

Modify

Field	Current	New
Syntax Parameters	**Usage Type —** Specifies the server usage type. Can be one of the following values: **login**, **802.1x** or **all**. If unspecified, defaults to **all**	**Usage Type —** Specifies the server usage type. Can be one of the following values: **login**, **dot.1x** or **all**. If unspecified, defaults to **all**
Description	Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks.	Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. Up to 4 RADIUS servers can be defined.

802.1x

Title	Description
Radius attributes relevant to 802.1x	The Radius attributes that are relevant to 802.1x functionality are: EAPMessage = 79, MessageAuthenticator = 80, State = 24, Class = 25.

Modified Commands in the CLI Reference Guide

clock summer-time

Under **User Guidelines** add the following:

The following steps must be completed before setting the summer clock:

3. Summer time configuration, for example: console(config)# clock summer-time recurring usa
4. Define Timezone, for example : console(config)# clock timezone 2 zone RADL
5. Set clock, for example: console# clock set 10:00:00 apr 15 2004

sntp anycast client enable

Update the command as follows:

Field	Current Guide	Change to:
Description	The **sntp anycast client** enable Global Configuration mode command enables anycast client. To disable the polling for SNTP broadcast client, use the no form of this command.	The **sntp anycast client enable** Global Configuration mode command enables anycast client. To disable the SNTP anycast client, use the no form of this command.

sntp client enable

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines	♦ Use the **sntp client enable** Global Configuration mode command to enable broadcast clients globally.	♦ Use the **sntp broadcast client enable** Global Configuration mode command to enable broadcast clients globally.

bridge address

Update the command as follows:

Field	Current Guide	Change to:
Syntax	**bridge address** *mac-address* {**ethernet** *interface* | **port-channel** *port-channel-number*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]	**bridge address** *mac-address* [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**] {**ethernet** *interface* | **port-channel** *port-channel-number*}

bridge aging time

Update the command as follows:

Field	Current Guide	Change to:
Syntax parameter	*seconds* — Time is number of seconds. (Range: 10 - **630** seconds)	*seconds* — Time is number of seconds. (Range: 10 - **360** seconds)

port security

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines	There are no user guidelines for this command.	Multiple hosts must be enabled.

show bridge address-table count

Update the command as follows:

Field	Current Guide	Change to:
In Example	Console# show bridge address-table count Capacity: 8192 Free: 8084 Used: 108 Static addresses: 2 Dynamic addresses: 97 Internal addresses: 9	Console# show bridge address-table count Capacity: 8192 Free: 8084 Used: 108 Static addresses: 2 Dynamic addresses: 97 Internal addresses: 9 **Secure addresses: 10**

show bridge multicast address-table

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines	There are no user guidelines for this command.	A MAC address can be displayed in IP format only if it is in the range of 0100.5e00.0000-0100.5e7f.ffff.

show ports security

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines	There are no user guidelines for this command.	If no parameters are entered, all entries are displayed.

clock summer-time

Update the command as follows:

Field	Current Guide	Change to:
Syntax Parameter	*week*— Week of the month. (Range: 1 - **4**, first, last)	*week*— Week of the month. (Range: 1 - **5**, first, last)

sntp broadcast client enable

Update the command as follows:

Field	Current Guide	Change to:
Dedscription	To disable the SNTP anycast client, use the **no** form of this command.	To disable the anycast client, use the **no** form of this command.

Mdix

Update the command as follows:

Field	Current Guide	Change to:
Syntax Parameter	**on—**Manual mdix	**on—**Enable mdi/mdix

port storm-control broadcast enable

Update the command as follows:

Field	Current Guide	Change to:
Syntax Parameter	**port storm-control broadcast enable** **no port storm-control broadcast enable**	**port storm-control broadcast enable**[**ethernet** *interface*] **no port storm-control broadcast enable** ♦ *interface*—A valid Ethernet port.

port storm-control broadcast rate

Update the command as follows:

Field	Current Guide	Change to:
Syntax Parameter	rate—Maximum kilobytes per second of broadcast and multicast traffic on a port. (Rate: 0 - 1488095)	♦ rate—Maximum kilobytes per second of broadcast and multicast traffic on a port. (Rate: 0 – 65535)
User Guidelines	The granularity is 1 - 64K packets. Note that if the rate is 0, broadcast packets are not forwarded.	Delete this guideline.
Example	console(config-if)# port storm-control broadcast rate 10	console(config)# port storm-control broadcast rate 10

show ports storm-control

Update the command as follows:

Field	Current Guide	Change to:
Example	Broadcast Storm control [kbytes/sec]	Broadcast Storm control [packets/sec]

clear host

Update the command as follows:

Field	Current Guide	Change to:
Example	The following example deletes entries from the host name-to-address cache.	The following example deletes **all** entries from the host name-to-address cache.

permit (management)

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines	The system supports up to 256 management access rules.	The system supports up to 128 management access rules.

show copper-ports tdr

Update the command as follows:

Field	Current Guide	Change to:
Example	The following example displays the last TDR (Time Domain Reflectometry) tests on all ports.	The following example displays the last TDR (Time Domain Reflectometry) tests on all copper ports.
	g5 Fiber - -	Delete.

Port monitor

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines		Add this extra bullet: ♦ Maximum number of supported source ports is 8 (Rx and Tx).

channel-group

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines	There are no user guidelines for this command.	For redundancy reasons, the LACP port channel can accept up to 16 ports but only 8 will be active at the same time.

wrr-queue bandwidth

Update the command as follows:

Field	Current Guide	Change to:
User Guidelines	♦ All 4 queues are participating excluding the queues that are assigned as expedite queues. The weights of these queues are ignored in the ratio calculation. ♦ All 4 queues participate in the WRR exclude the expedite queues, in which case the corresponded weight is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.	♦ All 4 queues are participating excluding the queues that are assigned as Strict Priority (SP) queues. The weights of these queues are ignored in the ratio calculation. ♦ All 4 queues participate in the WRR exclude the Strict Priority (SP) queues, in which case the corresponded weight is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.

rmon collection history

Update the command as follows:

Field	Current Guide	Change to:
Syntax Parameter	**owner** ownername—Records the RMON statistics group owner name. If unspecified, the name is an empty string.	**owner** ownername—Records the RMON statistics group owner name. If unspecified, the name is an empty string (Range: 0-20 characters).

switchport trunk allowed vlan

Update the command as follows:

Field	Current Guide	Change to:
Syntax Parameter	**switchport trunk allowed vlan** {**add** *vlan-list* | **remove** *vlan-list* } • *add vlan-list*—List of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.	**switchport trunk allowed vlan** {**add** *vlan-list/all* | **remove** *vlan-list/all* } ♦ *add vlan-list*—List of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs. The option *all*

	• *remove vlan-list*—List of VLAN IDs to remove. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designate a range of IDs.	adds all configured VLAN IDs. ♦ *remove vlan-list*—List of VLAN IDs to remove. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designate a range of IDs. The option *all* removes all configured VLAN IDs.

crypto certificate generate

Update the command as follows:

Field	Current Guide	Change to:
Syntax Parameter	crypto certificate [number] generate [key-generate [length]] [passphrase string] [cn common- name] [ou organization-unit] [o organization] [l location] [st state] [c country] [duration days]	crypto certificate [number] generate [key-generate [length]] [cn common- name] [ou organization-unit] [o organization] [l location] [st state] [c country] [duration days]
Syntax Parameter	**passphrase** string—Passphrase that is used for exporting the certificate in PKCS12 file format. If unspecified the certificate is not exportable. (Range: 8 - 96)	Delete the parameter

sntp broadcast client enable

Change a parameter description:

	Current Guide	Change to:
User Guideline	Use the sntp client enable Interface Configuration mode command to enable the SNTP client on a specific interface.	Use the sntp broadcast client enable Interface Configuration mode command to enable the SNTP client on a specific interface.

permit (management)

Change a parameter description:

	Current Guide	Change to:
User Guideline	The system supports up to 256 management access rules.	The system supports up to **128** management access rules.

radius-server host

Change a parameter description:

	Current Guide	Change to:
Syntax Parameter	♦ type—Specifies the usage type of the server. Can be one of the following values: login, **802.1x** or all. If unspecified, defaults to all.	♦ type—Specifies the usage type of the server. Can be one of the following values: login, **dot.1x** or all. If unspecified, defaults to all.
User Guidelines		Add: ♦ Up to 4 servers can be defined.

Deleted Commands

The following commands are documented but not supported in this release.

- default vlan-disable
- show vlan internal usage
- ip internal-usage-vlan

Modified Text

Under the heading Editing Features and sub-heading Terminal Command Buffer.

Current Guide	Change to:
The standard number of 10 commands can be increased to **256**.	The standard number of 10 commands can be increased to **216**.

Examples:

TAC_PLUS configuration

Note for $enab15$ user setup.
The following user is needed if a user is allowed to go from level 1 to a level 15.

Example.
logs into as user lever then goes to a exec user from console.

```
console>enable
enter password if console password id enable.

console#
 user = $enab15$ {
 default service = permit
 login = cleartext "15"
 service = exec {
 priv-lvl = 15
}
}
```

End of Release Notes