Firmware Version: 3.60.28
Prom Code Version: v1.0.1.05
Published: July 30, 2010

These release notes include important information about D-Link switch firmware revisions. Please verify that these release notes are correct for your switch:

- If you are installing a new switch, please check the hardware version on the device label; make sure that your switch meets the system requirement of this firmware version. Please refer to

- Revision History and System Requirement for detailed firmware and hardware matrix.

- If the switch is powered on, you can check the hardware version by typing "show switch" command or by checking the device information page on the web graphic user interface.

- If you plan to upgrade to the new firmware release, please refer to the Upgrade Instructions for the correct firmware upgrade procedure.

Content:

dlink green

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version	Note
Runtime: v3.60.28 Prom: v1.0.1.05	30-Jul-10	DGS-3100-24	A1, A2, B1	
		DGS-3100-24P	A1	
		DGS-3100-48	A1, A2, B1	
		DGS-3100-48P	A1	
		DGS-3100-24TG	A1, A2, B1	
Runtime: v3.50.23 Prom: v1.0.1.05	22-Mar-10	DGS-3100-24	A1, A2, B1	
		DGS-3100-24P	A1	
		DGS-3100-48	A1, A2, B1	
		DGS-3100-48P	A1	
		DGS-3100-24TG	A1, A2, B1	
Runtime: v3.00.43 Prom: v1.0.1.04	15-Aug-09	DGS-3100-24	A1, A2	Not compatible with hardware version B1
		DGS-3100-24P	A1	
		DGS-3100-48	A1, A2	
		DGS-3100-48P	A1	
		DGS-3100-24TG	A1, A2	
Runtime: v2.50.43 Prom: v1.0.1.01	25-Apr-09	DGS-3100-24	A1, A2	Not compatible with hardware version B1
		DGS-3100-24P	A1	
		DGS-3100-48	A1, A2	
		DGS-3100-48P	A1	
		DGS-3100-24TG	A1, A2	

Upgrade Instructions:

Caution1: The PROM version 1.0.1.01 works with firmware version 2.50.43 and PROM version 1.0.1.04 works with firmware version 3.00.43. DO NOT PROCEED the upgrading without verifying the PROM and firmware combination first. Direct upgrade from incorrect PROM and firmware combination is not suggested and may result in unknown issues.

Caution2: The PROM version 1.0.1.05 with firmware version 3.50.23 or above works with hardware version B1, which supports D-Link Green function.
DO NOT DOWNGRADE the firmware to the version prior than 3.50.23 on B1 hardware version. The switch will not work.

Caution3: All functions can work well except the Green features if upgrading A1 & A2 hardware versions to firmware 3.50.23 or above with PROM 1.0.1.05.

PLEASE DO NOT REBOOT THE SWITCH BEFORE YOU COMPLETE THE UPLOADING FOR BOTH PROM AND FIRMWARE.

dlink green

D-Link switches support firmware upgrade via TFTP server. You can download the firmware from D-Link web site http://www.dlink.com.au , and copy the downloaded firmware to the TFTP server folder. Please make sure that the TFTP server is accessible from the switch via networks.

Upgrade using CLI (serial port)

Connect a workstation to the switch console port and run any terminal program that can emulate a VT-100 terminal. The switch serial port default settings are as follows:

- Baud rate: **9600**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**

The switch will prompt the user to enter his/her username and password. It should be noted that upon the initial connection, there is no username and password by default.

To upgrade the switch's firmware and PROM, execute the following commands:

Command	Function
download [firmware_fromTFTP <ipaddr> <path_filename 64> {image_id <int 1-2>}]	Download Runtime firmware file from the TFTP server to the switch.
config firmware image_id <1-2> [delete | boot_up]	Change the boot up image file.
show firmware_information	Display the information of current boot image and configuration.
download [boot <ipaddr> <path_filename 1-64>]	Downloads a boot (PROM) file from a TFTP server.
reboot	Reboot the switch.

Example:

```
1.   DGS-3100# download firmware 172.17.5.124 dgs_31xx_gen-36028.ros
     08-Feb-2000 23:10:57 %COPY-I-FILECPY: Files Copy - source URL tftp://172.17.5.12
     4/dgs_31xx_gen-36028.ros destination URL Unit all flash://image
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!08-Feb-2000 23:13:56 %CO
     PY-N-TRAP: The copy operation was completed successfully
     !
     Copy: 4387258 bytes copied in 00:03:00 [hh:mm:ss]

     DGS-3100#

2.   DGS-3100# show firmware information
```

dlink green

```
Command: show firmware information

Unit  Image      Version         Update Time
----  ---------- --------------- ---------------
1     *1         3.60.28         08-Jun-2010 11:09:16
1     2          3.50.23         05-Mar-2010 00:42:47


"*" designates that the image was selected for the next boot
```

3.   DGS-3100# download boot 172.17.5.124 dgs_31xx_boot-10105.rfb
     08-Feb-2000 23:25:10 %COPY-I-FILECPY: Files Copy - source URL tftp://172.17.5.12
     4/dgs_31xx_boot-10105.rfb destination URL Unit all flash://BOOT
     !!
     !!!!!!!!!!!!!!!!!!!!!!!08-Feb-2000 23:25:49 %COPY-N-TRAP: The copy operation was
     completed successfully
     !
     Copy: 524304 bytes copied in 00:00:39 [hh:mm:ss]

4.   DGS-3100# reboot
     This action may take a few minutes
     You haven't saved your changes. Are you sure you want to continue ? (Y/N)[N] Y
     Are you sure you want to proceed with system reboot now? (Y/N)[N] Y

New Features:

Firmware Version	New Features
v3.60.28	1 Time-based PoE
	2 Dynamic VLAN Assignment
	3 Voice VLAN
	4 IPv6 ACL
	5 Cable Diagnostics
	6 Password Encryption
	7 Display statistics information of error packets on CLI and Web GUI
	8 Be able to configure serial port's parameters (baud rate, time out) via Web GUI
	9 Be able to login switch with blank user name and password
	10 Link Aggregation algorithm improvement. l Based on source and destination MAC addresses l Based on source and destination IP addresses l Based on IP and MAC's source and destination addresses
	11 Configuration filtering: Filter the configuration file with specified key word while displaying it on CLI
	12 All ports can be the source port in Port Mirror function
	13 When broadcast storm reaches the configured threshold, switch will

	disable the port and send trap to NMS
v3.50.23	1 Support D-Link Green feature l Power Saving by Link Status l Power Saving by Cable Length 2 Support Smart Fan for DGS-3100-24/48/24TG 3 Support 'show tech-support' command 4 Support Safari web browser version 4 5 Be able to configure static ARP entry for multicast MAC address 6 The default VLAN can be configured as the Guest VLAN 7 Ports can be removed from default VLAN 8 Be able to display system uptime in CLI console 9 Be able to delete firmware image 10 Be able to change the VLAN name via CLI command 11 Displaying the mainboard's temperature with B1 hardware version. 12 Be able to enable Trusted Host by applications 13 System MAC will be displayed in FDB table
v3.00.43	1 ARP Spoofing Prevention 2 DHCP Relay with Option 82 3 Asymmetric VLAN 4 LLDP disabled by default 5 Be able to configure static ARP entry for multicast MAC address 6 Display the real port count when querying RFC1213 ifTable 7 Be able to configure Traffic Segmentation with multiple source and forwarding ports 8 The target mirror port can forward traffic and be assigned to default VLAN 9 Provide more detailed information while executing 'show safeguard' command 10 Be able to display the default configuration of all features 11 Support three parameters for Port Security's Lock Address Mode : l Permanent l DeleteOnTimeout l DeleteOnReset 12 When enabling SSH, Telnet will be disabled 13 Enhance VLAN Trunking to support up to 48 uplink ports

	14 Change the Web UI login behavior for user level authorization
	15 Expand the Trust Host number to 10 and support the Trust Host Network feature
	16 The Web UI will display the trap interval in Port Security Page.
	17 Be able to configure Destination Lookup Failure (DLF) for ports
	18 Be able to configure the recovery time when port is shut down by loop
v2.50.43	1 MLD Snooping v1 and v2
	2 Time Based ACL
	3 Enable/Disable Telnet Server
	4 LLDP
	5 IGMP Querier
	6 Display switch's serial number on the Web UI and CLI
	7 VLAN Trunking When enabling this feature, DGS-3100 will pass the traffic with unknown VID to VLAN trunking port instead of dropping it.
	8 Be able to configure Traffic Segmentation on Management VLAN
	9 Be able to configure ACL on Link Aggregation Port
	10 Be able to configure port speed and duplex mode on a Link Aggregation Trunk channel group
	11 The EAP packet from clients will be flooded by default
	12 Be able to configure port without assigning stacking ID
	13 Keep the default route setting when management IP changed
	14 The unregistered multicast group will be flooded by default
	15 Disable the Spanning Tree Protocol by default
	16 When loop is detected, the port will be shut down and after a period of time, the port will automatically recover
	17 Change the port displaying format. The above figure is the old format and the below one is the latest format.

```
PORT_LIST        portlist
ch1              ch1
ch2              ch2
ch3              ch3
```

```
| 9600
DGS-3100# config stp ports
Command:  config stp ports

  all                   all
  PORT_LIST             portlist/channel group
DGS-3100# config stp ports ▐
```

18 Support new parameters for "config access_profile" command

l   Support channel interface parameter: ports [<portlist> | <ch1-32>]

l   Support time range parameter: {time_range <range_name 32>}

19 Support new parameter for "config ipif system" command

l   Support VLAN name parameter: {dhcp | vlan <vlan_name 32>}]

20 Support new parameter for "show router_port" command

l   Support displaying the forbidden port:
{vlan <vlan_name 32> | static | dynamic| forbidden}

21 Modify the parameter for "config traffic_segmentation" command.

l   Support port list for source port: [<portlist> | <ch1-32>]

v2.00.47	Default VLAN can be configured as Tagged VLAN
v1.00.36 (DGS-3100-24/48) v1.00.37 (DGS-3100-24P/48P)	First release. For supported features, please refer to the product specification and manuals for details.

Changes of MIB & D-View Module:

The new features of MIB file are also included in the corresponding D-View module. Please download the D-View module from http://tsd.dlink.com.tw. For detailed changes of MIB content, please refer to the modification history in each MIB file.

Firmware Version	MIB File	New Features
v3.60.28	tbi.mib	Support time range configuration
	RFC2011.mib	A standard MIB to manage IP and ICMP implementation
	RFC2013.mib	A standard MIB to manage UDP implementation
	DLINK-3100-stormctrl-mib.mib	Support new action types for storm control ('drop', 'drop and shutdown')

	DLINK-3100-traps-mib.mib	Support trap notification for storm control
	rlPoe.mib	Support Time-based PoE
v3.50.23	mnginf.mib	Support the Ping application in Trusted Host
	rldeleteimg.mib	Support firmware image deletion
	rlgreeneth.mib	The Green Ethernet MIB
v3.00.43	rlinterfaces.mib	Support Port Security's new parameters
	rlphysdescription.mib	Add new parameters to support LLDP Manufacturer and Model name information
	rlSafeGuard.mib	Change the threshold limitation from 99% to 100%
	rlvlan.mib	Support Asymmetric VLAN
	rfc2674.mib	This MIB file is replaced by p-bridge-mib.mib and q-bridge-mib.mib
	rlimpb_arp_inspection.mib	Support ARP Spoofing Prevention
	rlimpb_features.mib	
	rlimpbmng.mib	
	rldlf.mib	Support DLF feature
	rltrafficsegmentation.mib	Support Traffic Segmentation
v2.50.43	Banner.mib	Configurable banner information
	inet-address-mib.mib	Replace RFC2851.mib due to the changes of standard. This MIB module defines textual conventions for representing Internet addresses. An Internet address can be an IPv4 address, an IPv6 address, or a DNS domain name.
	lldpextdot3.mib	Support LLDP
	lldpextmed.mib	
	diffserv-dscp-tc-rfc3289.txt	
	rllldp.mib	

	rlphysdescription.mib	
	rlVlanTrunking.mib	Support VLAN Trunking
	ianaifty.mib	Modify this mib file to follow RFC 1573 which is used as the syntax of the ifType object in the (updated) definition of MIB-II's ifTable.
	rlinterfaces_recovery.mib	Support the recovery option when loop is detected
	policy.mib	Support time-based ACL configuration
	rlbrgmulticast.mib	Support IGMP Snooping querier
	rlSafeGuard.mib	Support configuring threshold
v2.00.47	None	
v1.00.36 (DGS-3100-24/48) v1.00.37 (DGS-3100-24P/48P)	First release. Please refer to datasheet for supported SNMP MIB files.	

Changes of Command Line Interface:

The section below only shows command line changes that may bring backward compatibility issues with configuration settings for previous version of firmware.
Any new feature commands that do not have backward compatibility issues are not included in the below section.

Fireware Version	New Features
v3.60.28	1 Modify "config traffic control" command to support Broadcast Storm Control feature l config traffic control {[<portlist> | all] state [enable | disable] | storm_type [broadcast | multicast_broadcast | dlf_multicast_broadcast] threshold <int 3500-1000000> **action [drop | shutdown] time_interval <value 5-30>**
v3.50.23	1 Modify "config firmware" command to support deleting image feature l config firmware [**delete** | **boot_up**] {unit <unit_id 1-6>} image_id <init 1-2> 2 Modify "create trusted_host" command to support Trusted Host by application feature l create trusted_host <ipaddr>{network <network_address>} {**application [telnet | ssh | snmp | http | https | ping | all**}

	1	Modify Safeguard Engine command to support defining threshold
		l config safeguard_engine {state [enable | disable] | {rising <value 20-100> | falling <value 20-100>}}
	2	Modify the command "show_safeguard" to "show safeguard_engine"
	3	Remove "enable safeguard" and "disable safeguard" commands
	4	Modify Traffic Segmentation command to support configuring multiple source and forwarding ports
		l config traffic_segmentation [<portlist> | <ch1-32>] forward_list [<portlist> | <ch1-32>]
v3.00.43	5	Modify Spanning Tree command to support configuring recovery timer for ports which are shut down by loop
		l config stp {maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-10> | forwarddelay <value 4-30>| fbpdu [enable | disable] **lbd [enable | disable]** | **lbd_recover_timer [<value 30-86400>]**}
	6	Modify Port Security command to support lock_address_mode's new parameters
		l [<portlist> | all] {admin_state [enable | disable] | max_learning_addr <int 1-64> | **lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]** | trap <interval 1-1000000>}
	1	Change the command "config guest vlan" to "create 802.1x guest_vlan"
	2	Change the command "config guest_vlan ports" to "config 802.1x guest_vlan ports"
	3	Change the command "show guest_vlan" to "show 802.1x guest_vlan"
	4	Change the command "config rate_limit" to "config bandwidth_control"
	5	Change the command "show rate_limit" to "show bandwidth_control"
	6	Modify "config snmp system_contact" command's parameter
		l Describe the allowable character number: <sw_location **0-31**>
v2.50.43	7	Modify "config snmp system_name" command's parameter
		l Describe the allowable character number: <sw_name **0-31**>
	8	Change the command "show cpu utilization" to "show utilization" and also add one more parameter
		l Support two parameters: [**ports** | cpu]
	9	Modify the parameter for "traceroute" command.
		l change the packet size from "[size 40-1500]" to "[size 40-**1472**]"

v2.00.47	None
v1.00.36 (DGS-3100-24/48) v1.00.37 (DGS-3100-24P/48P)	First release

Problem Fixed:

Firmware Version	Problems Fixed
v3.60.28	1 The "Time Zone Offset" cannot be changed via Web GUI but there is no problem for CLI command. (DRU20100318000003) 2 User cannot add a VLAN name with space in CLI but no problem for Web GUI (DI20100209000008)
v3.50.23	1 The "Port ID" and "Port ID Subtype" in the LLDP TLV information display Hex string in Web UI instead of displaying alphanumeric one. (DI20090330000015) 2 The stack cannot be established due to that the switch's MAC overlapped. (DI20091208000009)
v3.00.43	1 If user changes switch's unit ID to 2 and queries the ifTable MIB file, system will hang up. 2 When user tries to disable Telnet via the Web UI while running the command "show configuration running", the Telnet session will not be disabled and there is no warning message, either. 3 When user tries to configure 128.0.0.0 subnet mask in Trusted Host feature, the CLI will accept the command but Web UI will display "128.0.0.0 is not a valid IP mask" warning message. 4 In Port Security, when user changes the setting of "lock_address_mode", the value of "admin_stat" will be changed, too.
v2.50.43	1 When executing the command 'configure ipif' and key in the '?' to query the next available parameter, it will display 'system' instead of 'System'. 2 Users can only open two web sessions in stacking architecture. 3 Users can configure the stacking port as the LACP port. 4 When configuring Trust Host, Syslog, SNMP, SNTP, Radius and ARP features; Illegal IP address is acceptable without any error or warning message. 5 When user configures port security with trap enabled on specific ports via CLI and afterwards configures port security on other ports with no trap enabled via Web UI, using the 'show port_security' or 'show configuration running' commands on CLI, the user can see that the trap appears also

on the ports configured by the Web (without a trap)

6   When user tries to show VLAN, STP and GVRP information via CLI, the 'q' button doesn't interrupt the displaying when type it.

7   The QoS is not working properly when using queue 3 across the stack. It happens in strict priority and also in WRR, if the user does not use queue 3, everything is working fine.

8   A fatal error happened when there are multiple HTTP connections sending large files at the same time (DI20080627000006).

9   Sometimes when rebooting the Master or Backup Master switch in a stack, the stacking may crash (DI20081106000013).

10 When configuring the ACL function with more than 100 access IDs, the system will display a warning message "Exceeded the maximum ACE allowed in the system". However, the ACL rules are not running out actually (DI20081028000024).

11 When users try to login the Web UI with 'user' privilege, the system will display an "Invalid username or password" error message (DI20080630000017).

12 When a client sends an IGMP leave request to one multicast group, another group for that user will be disconnected, too (DI20081001000004).

13 When users configure MSTP feature, MSTP can not be configured for non-existing VLAN (DI20080820000010).

14 Fix the problem of incorrect statistics number of Port Utilization (DI20080807000011).

15 When users connect several clients on several Slave switches and also enable flow control. If clients overload the stacking bandwidth to Master switch, the stacking may break and all switches will reboot to re-build the stacking.

16 When executing "show port" command in a single switch, DGS-3100 will always display the maximum interfaces (48 ports multiply with six switches in a stack).

v2.00.47	1	In current design, the ACL was port based and only support 128 access rules for whole system (though in spec we stated 240 rules support and each rule is system-based) For example, if you configure one ACL in stacking mode and apply it to more than 128 ports, you'll have problem for this function. With firmware version 2.00.47, if user applies a rule for the whole stacking, it will only be counted as 1 rule. For the detail of new ACL mechanism, please refer to the session, "Notes about ACLs capacity in the DGS-3100 Series", in user manual.
	2	Current system IP only supports classful IP address, such as class A, B or C with associate subnet mask such as /8, /16 or /24, if you configure Class C IP address with wrong subnet mask, say /16(255.255.0.0), you will receive an error message saying that the mask is illegal.
	3	When user configures ACL to change the 802.1p packet priority, the system will not map the packet to the right queue.

	4	When user is copying and pasting a group of long commands, some of the commands will not work.
	5	When typing: 'show fdb aging time' and '?' afterwards system will display other options. Actually, there shouldn't be additional values in this command
	6	When user deletes access profile through the web, the profile details will remain.
	7	Users can not configure more than 5 user accounts via the Web UI.
	8	When user configures ACLs on the Web UI, the system will not check the TCP Flag parameter which is configured as "unset (0)" and will only check the parameter "set (1)".
	9	When pasting commands, the prompt will be displayed in the wrong position.
	10	When configuring MAC_base_access_control and copying the configuration file to TFTP server. The function will not work when user restore the configuration file back to the switch.
	11	If the user configures a port to guest VLAN and also configures the port as untagged in the same VLAN, the port will not belong to any VLAN after the user changes the "port control" to "force authorize" state..
	12	When user tries to create an IP access profile with mask of all "0" The system will accepted it.
v1.00.36 (DGS-3100-24/48) v1.00.37 (DGS-3100-24P/48P)	First release	

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues	Workaround
v3.60.28	None	
v3.50.23	None	
v3.00.43	The LLDP TLV information, the "Port ID" and "Port ID Subtype", displays Hex string in Web UI instead of displaying alphanumeric one. (DI20090330000015)	User can see alphanumeric string in CLI.
v2.50.43	None	
v2.00.47	1 It is impossible to activate the third web session	Two web sessions work properly within the stack, in standalone mode there is no problem at all.
	2 It is possible to configure the stacking port (port 49, 50) as LACP port.	The stacking port will still be a stacking even though it was

			configured as a LACP port. The LACP configuration does not take effect.
	3	The user can configure illegal IP address for several features, like "Trust Host", "Syslog", "SNMP", "SNTP", "Radius" and "ARP", without any warning message.	There is no problem if the user configures correct IP addresses
	4	When configuring "ipif", the switch displays ''system'' but not ''System''	It is displaying problem and no effect on the functionality.
	5	Dynamic VLAN is not displayed in the VLAN page when the browser is in security level high or medium-high.	It was tested with IE7, it works fine if lowering browser's security level
	6	If the user configures port security on specific ports via the CLI and configures trap on these ports and afterwards configures port security on other ports from the web without a trap, using the show port_security and show configuration running commands on CLI, the user can see that the trap appears also on the ports configured by via the web (without a trap)	None
	7	When user tries to show VLAN, STP and GVRP information via CLI, the 'q' button does not interrupt the displaying when you type it. For example: when you typed "show GVRP ?", the PORTLIST + LAG list was printed, typed "q" to stop displaying but the rest of the LAGs were printed any way.	It does not affect the switch functionality.
	8	QoS does not work properly when using queue 3 across the stack. It happens in strict priority and also in WRR. When the user does not use queue 3 everything works fine.	Do not use queue 3 under stacking topology

* D-Link tracking number is enclosed in ()

Related Documentation:

- DGS-3100 Series User Manual v3.6
- DGS-3100 Series CLI Manual v3.6
- DGS-3100 Series Hardware Installation Guide v3.5