



Firmware Version: v2.50.43
Prom Code Version: v1.0.1.01
Published: 2009/6/10

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

- w 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 detail firmware and hardware matrix.
- w If your switch is 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.
- w If you plan to upgrade to the new firmware release, please refer to the [Upgrade Instructions](#) for the correct firmware upgrade procedure.

For more detailed information regarding our switch products, please refer to [Related Documentation](#).

You can also download the switch firmware, D-View modules and technical documentation from <http://tsd.dlink.com.tw>.

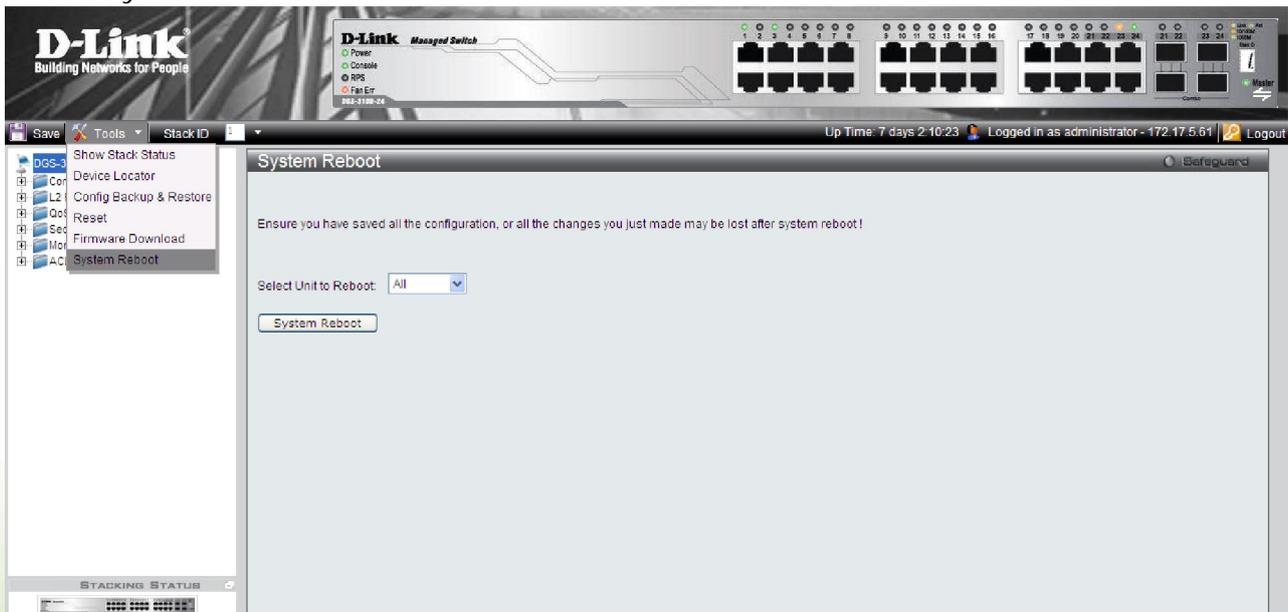
Content:

Revision History and System Requirement	2
Upgrade Instructions.....	2
Upgrade using CLI	2
Upgrade using Web-UI	3
New Features.....	5
Changes of MIB & D-View Module.....	6
Changes of Command Line Interface.....	7
Problem Fixed	8
Known Issue.....	10
Note	11
Related Documentation	11

6. If you choose HTTP download, enter the firmware file name and associated path on your computer. If you choose TFTP download, enter the TFTP server IP and the firmware file name.
7. If the switch is under stacking mode, select the unit ID 'all' to update the firmware for all switches in the stack.
8. Click "Download" button.
9. Wait until the file Transfer status becomes "Copy Finished".



10. Reboot the system by clicking **Tools > System Reboot** from the banner and click "System Reboot" button to reboot the switch.



New Features

Firmware Version	New Features
v2.50.43	<ol style="list-style-type: none"> 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. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre> PORT_LIST portlist ch1 ch1 ch2 ch2 ch3 ch3 </pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre> 9600 DGS-3100# config stp ports Command: config stp ports all all PORT_LIST portlist/channel group DGS-3100# config stp ports </pre> </div> 18. Support new parameters for "config access_profile" command

	<ul style="list-style-type: none"> I Support channel interface parameter: ports [<portlist> <ch1-32>] I Support time range parameter: {time_range <range_name 32>} <p>19. Support new parameter for "config ipif system" command</p> <ul style="list-style-type: none"> I Support VLAN name parameter: {dhcp vlan <vlan_name 32>} <p>20. Support new parameter for "show router_port" command</p> <ul style="list-style-type: none"> I Support displaying the forbidden port: {vlan <vlan_name 32> static dynamic forbidden} <p>21. Modify the parameter for "config traffic_segmentation" command.</p> <ul style="list-style-type: none"> I 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 on <http://tsd.dlink.com.tw>.

Firmware Version	MIB File	New Features
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	
	rphysdescription.mib	
	rVlanTrunking.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
	rISafeGuard.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
v2.50.43	<ol style="list-style-type: none"> 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 Describe the allowable character number: <sw_location 0-31> 7. Modify "config snmp system_name" command's parameter 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 Support two parameters: [ports cpu] 9. Modify the parameter for "traceroute" command. change the packet size from "[size 40-1500]" to "[size 40-1472]"
v2.00.47	None
v1.00.36 (DGS-3100-24/48)	First release

v1.00.37

(DGS-3100-24P/48P)

Problem Fixed

Firmware Version	Problems Fixed
	<ol style="list-style-type: none"> 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.
v2.50.43	<ol style="list-style-type: none"> 8. A fatal error happened when there are multiple HTTP connections sending large files at the same time (DI2008062700006). 9. Sometimes when rebooting the Master or Backup Master switch in a stack, the stacking may crash (DI2008110600013). 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 (DI2008102800024). 11. When users try to login the Web UI with 'user' privilege, the system will display an "Invalid username or password" error message (DI2008063000017). 12. When a client sends an IGMP leave request to one multicast group, another group for that user will be disconnected, too (DI2008100100004). 13. When users configure MSTP feature, MSTP can not be configured for non-existing VLAN (DI2008082000010). 14. Fix the problem of incorrect statistics number of Port Utilization (DI2008080700011). 15. When users connect several clients on several Slave switches and also enable flow control. If clients overload the stacking bandwidth to Master

	<p>switch, the stacking may break and all switches will reboot to re-build the stacking.</p> <p>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).</p>
<p>v2.00.47</p>	<ol style="list-style-type: none"> 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)	First release
v1.00.37 (DGS-3100-24P/48P)	

Known Issue

Firmware Version	Issues	Workaround
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
v2.00.47	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	Do not use queue 3 under

	happens in strict priority and also in WRR. When the user does not use queue 3 everything works fine.	stacking topology
--	---	-------------------

Note

Firmware Version	Note
v2.50.43	None
v2.00.47	<ol style="list-style-type: none"> 1. DGS-3100-24TG can work with firmware version 2.xx.xx. If user loads the firmware version 1.xx.xx will result in wrong behavior of the switch 2. The ACL architecture in version 2.xx.xx was different than version 1.xx.xx, the user is required to upload the configuration file from the device while running the previous version, then upgrade the firmware to version 2.00.47, reset the switch and then download the configuration file back to the switch 3. Since TCP/UDP port mask functions in Access profile has bugs in version 1.00.xx and be solved in current version, the user needs to configure it again with latest software version to operate it. 4. In firmware version 1.xx.xx, there was a bug that the TCP/UDP ports in access profile were in hexadecimal instead of decimal value and this bug fixed in version 2.xx.xx. Now the TCP/UDP port value entries are in decimal and not hexadecimal. However, if user upgraded from previous version (1.xx.xx) to current version, the value will be retained in hexadecimal. The user need to re-configure the ACL which use the TCP/UDP 5. In firmware version 1.xx.xx, user can configure up to 4 Radius/Tacacs servers which should be 3 servers for each type in the original spec. It was modified in firmware version 2.xx.xx, only 3 servers can be configured for each type. The user needs to reduce the number of server before he/she restores the file to firmware version 2.xx.xx. 6. In version 1.xx.xx, user didn't need to configure priority to Tacacs server. However, in version 2.xx.xx, the priority is required. The user needs to add the priority before he/she restores the file to firmware version 2.xx.xx.
v1.00.36 (DGS-3100-24/48)	None
v1.00.37 (DGS-3100-24P/48P)	

Related Documentation

DGS-3100 Series User Manual v2.40
DGS-3100 Series CLI Manual v2.20