Firmware Version: v2.50.B51
Prom Code Version: V1.10.B09
Published: 2010/6/3

These release notes include important information about D-Link DGS-3600 series 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:

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

- for the correct firmware upgrade procedure.

For more detailed information regarding DGS-3600 series switch products, please refer to **Error! Reference source not found.**.

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

Firmware Version	Date	Model	Hardware Version
Runtime: v2.50.B51 Prom: v1.10.B09 (middle code)	2010/6/3	DGS-3612	A1
		DGS-3612G	A1
		DGS-3627	A1
		DGS-3627G	A1
		DGS-3650	A1, A2
Runtime: v2.50.B25 Prom: v1.10.B09	2009/1/8	DGS-3612	A1
		DGS-3612G	A1
		DGS-3627	A1
		DGS-3627G	A1
		DGS-3650	A1, A2
Runtime: v2.40.B19 Prom: v1.10.B09	2008/2/5	DGS-3612	A1
		DGS-3612G	A1
		DGS-3627	A1
		DGS-3627G	A1
		DGS-3650	A1, A2
Runtime: v2.20.B38 Prom: v1.10.B09	2007/8/10	DGS-3612G	A1
		DGS-3627	A1
		DGS-3627G	A1
		DGS-3650	A1, A2
Runtime: v1.00.B66 Prom: v1.10.B06	2006/9/22	DGS-3627	A1
		DGS-3627G	A1
		DGS-3650	A1

Upgrade Instructions:

Caution: This version is only the middle code for fixing the issue - if the size of the next firmware is more then 4M, it can't upgrade from V2.50B25 or previous versoin to this firmware directly .

D-Link switches support firmware upgrade via TFTP server. You can download the firmware from D-Link web site http://tsd.dlink.com.tw, 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: **115200**
- 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 firmware, execute the following commands:

Command	Function
download firmware_fromTFTP <ipaddr> <path_filename 64> <drive_id> <pathname 64>	Download firmware file from the TFTP server to the switch.
config firmware <drive id> <pathname 64> boot_up	Change the boot up image file.
show boot_file	Display the information of current boot image and configuration.
reboot	Reboot the switch.

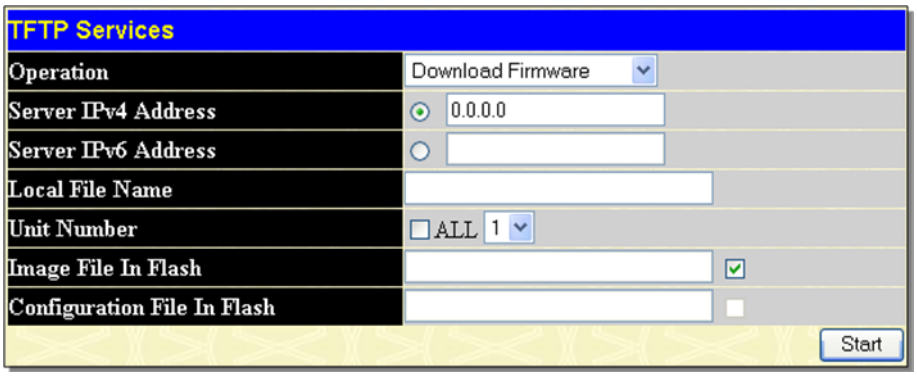
Example:

```
The switch:5# download firmware_fromTFTP 10.53.13.201 c:\ R280B31.had c:\ firm1
Command: download firmware_fromTFTP 10.53.13.201 c:\ R280B31.had c:\ firm1

Connecting to server.................Done.
Download firmware...................Done.  Do not power off!
Upload file to FLASH……..Done.

The switch:5# config firmware c:\ firm1\ R280B31.had boot_up
Command: config firmware c:\ firm1\ R280B31.had boot_up

Success.

The switch:5# show boot_file
Command: show boot_file
-------------------------------------------------------
 Unit ID : 1
 Boot up firmware image : C:\ R280B31.HAD
 Boot up configuration file: C:\STARTUP.CFG
 -------------------------------------------------------

The switch:5# reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y|n) y
Please wait, the switch is rebooting...
```

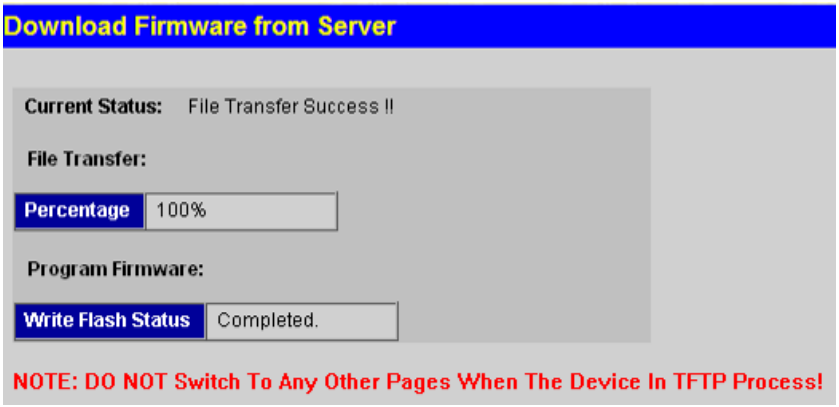
Upgrading by using Web-UI

1. Connect a workstation installed with java SE runtime environment to any switch port of the device.
2. Open the web browser from the workstation and enter the IP address of the switch. The switch's default IP address is 10.90.90.90.
3. Enter administrator's username and password when prompted. It should be noted that the username and password are blank by default.

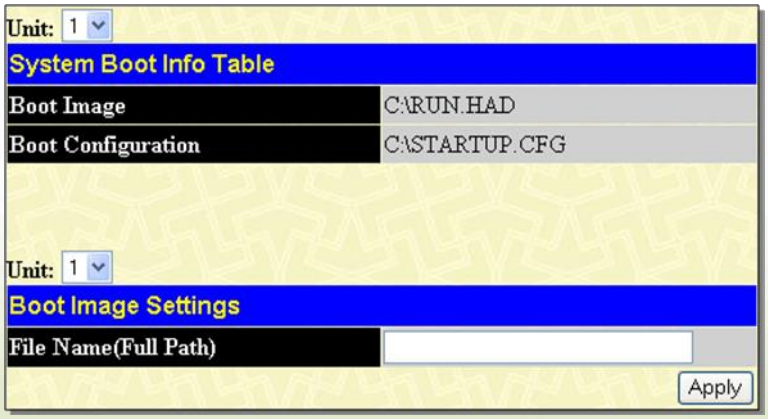
To update the switch's firmware or configuration file, click **Administration > TFTP Services** in function tree.



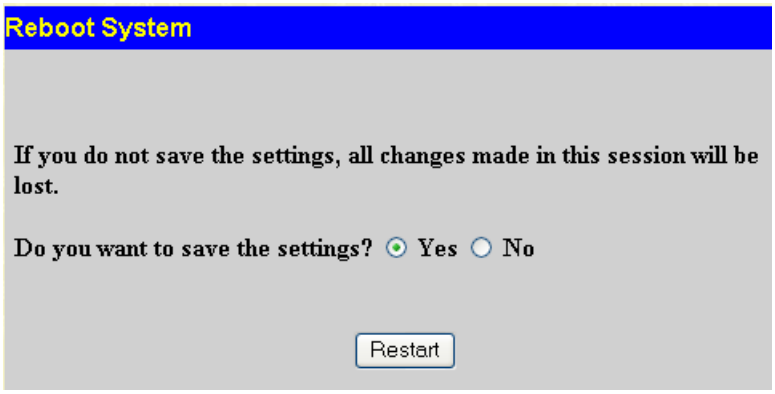
4. Select Download Firmware in **Operation.**
5. Select the type (IPv4 or v6) of IP address of the TFTP server and entering the IP address.
6. Enter the firmware file name which located on TFTP server on **Local File Name**.
7. If the switch is under stacking mode, select the unit ID that you would like to upgrade the firmware.
8. Entering the path you would like to store the firmware file in **Image File In Flash**. For example C:\firm1.
9. Enter "Start" button.
10. Wait for file Transfer to reach 100% and program firmware status completed.



11. To select the image which you want to boot up while the switch reboots next time, click **`Administration > File System Services > System Boot Information`** in function tree



12. Enter the complete path/file name and click Apply. For example C:\firm1\R280B31.had.
13. Reboot the system.



New Features

Firmware Version	New Features
v2.50.B51	1. Port Security max_learning_addr changed from 16 to 64. 2. IGMP source check : check the subscriber source IP when an IGMP report or leave message received 3. Link aggregation port can be set as RSPAN target port for CLI
v2.50.B25	4. Multicast static route 5. MAC-based access control 6. MAC-based VLAN 7. Loopback Detection (LBD) 4.0 8. Telnet client support 9. DHCP server screening 10. Proxy ARP 11. Support MTU configuration on IP interface 12. RSPAN 13. Per port configurable MDI/MDIX auto negotiation 14. L2 Protocol Tunneling (L2PT) 15. Selective QinQ 16. Serial number display support (Applicable from shipment loaded with this firmware) 17. Change floating static route behavior so that the primary route always has higher priority 18. OSPF ECMP route flag (Enable/Disable capability) 19. Add replace DSCP tag option on Ethernet type of ACL function 20. Change STP port forward BPDU default state to disabled 21. NAP-DHCP environment support 22. Show Fan status (Fan Status log and trap)
v2.40.B19	1. Port link up/down trap 2. Null interface for CLI 3. LLDP 4. Gratuitous ARP trap/log 5. Three-Level User Account 6. Allow the option to enter not only VLAN name but also VID in "show fdb VLAN" command 7. Error message to describe the naming rule of flash file system if user input the illegal file name

	8. VLAN PVID auto assignment (to solve this issue that the PVID will not change with the 802.1Q untagged port setting raised in R2.2) 9. Show VLAN by VID 10. Add PIM Sparse-Dense Mode for CLI 11. SNMP state can be enable and disable 12. Support new model DGS-3612
v2.20.B38	1. Physical Stacking 2. Trunking/Mirroring across stack 3. Mirroring ACL mode 4. 802.1v protocol VLAN enhancement 5. ISM VLAN (Only for standalone mode) 6. Double VLAN 7. IPv6 Floating Static Route 8. Secondary default route 9. OSPF Equal Cost Route 10. Multi Path Routing 11. Enlarge IP interface to 256 (per device/per VLAN) 12. IPv6 Ready Logo Phase 1 13. PIM SM 14. ACL Based on User Defined Packet Content 15. Web-based Access Control (WAC) 16. sFlow 17. DHCP Server 18. ACL Statistic
v1.00.B66	First release, please refer to datasheet and manual for detail function supported

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.B25	Genmgmt.mib	1. Add object agentFDBClearAllState for clear FDB table function 2. Add object agentARPClearAllState for clear ARP table function
	MldSnp.mib	1. Add object swMldSnpForwardingTable for show MLD snooping FDB function
	PIM-SM.mib	1. Add value "dynamic" at object swPimRPSetType to display dynamic rpset.
	rfc2737.mib	1. Add RFC2737 Entity MIB
v2.40.B19	Show memory utilization in MIB	
V2.20.B38	rfc2863.mib	1. Add RFC2863 IF MIB
v1.00.B66	First release, please refer to datasheet for detail MIB supported	

Problem Fixed

Fixed Revision	Troubled Version	Problems
v2.50.B51	v2.50.B25	**1. If the size of the next firmware is more then 4M, it can't support to upgrade to this firmware directly.** 2. Telnet into IX2000(router) via DGS-3650 successfully, but it needs to spend a long time to logout (about 1 minute) (DI20091013000002) 1. When using RIP to learn the dynamic routing entry, the subnet mask becomes 32. But the correct one should be 24. (DI20090910000012) 2. The user can not configure the VLAN forbidden ports with untagged member ports together via SNMP. (DI20100129000019) 3. When the master unit's power is cut off, the stacking switch doesn't respond SNMP Get Request correctly. Even if the Unit1's power is cut off and Unit2 become the master unit, the Unit1's port information can be seen. (DI20091217000006) 4. The DHCP clients sometimes will fail to get the IP address from DHCP server, but 2.40B19 does not have such issue. (DI20090519000007) 5. Plug/unplug the link aggregation member port, SNMP host can not receive SNMP trap. (DI20090924000017)
v2.50.B25	v2.40.B19	1. Sometimes when STP topology changes, the ipfdb table is not correctly updated and reflected. 2. Sometimes in Firefox v3.0.1 for SIM management, the position of the UI is not aligned properly. 3. When accessing switch Web UI via Firefox 3.0.1, the browser cannot refresh by pressing F5. 4. Firefox 3 cannot access switch Web UI correctly via SSL. 5. Openssh 5.1 software will sometimes cause the switch to go into exception mode. 6. Sometimes when IMPB DHCP snooping is enabled and connected to NetScreen 204 DHCP server, the switch fails to create DHCP snooping binding entry and block the client's MAC address. 7. Sometimes DES-3500 series cannot function properly with DGS-3600 series under SIM management. 8. Sometimes when MSTP is enabled and MSTP instances are configured, the computer will lose visibility to the switch. 9. Sometimes stacking member ports are not able to issue "clear counter ports" command. 10. After setting the bandwidth control on ports, the first 1 second still has burst traffic. 11. Ipfdb will not update when running VRRP + STP and also the STP topology has been changed at the same time 12. New members cannot join the stack after backup master takes over the job of stacking master 13. OSPF neighbor is unstable when enabling LACP in stacking mode 14. In some special environment, running OSPF causes high CPU utilization. 15. In some special network topology, OSPF will reboot every 10 minutes 16. F/W upgrade will fail if the file name contains more than one "dot", for example "2.40B30.had"

		17. PIM does not work when System ipif is disabled 18. DGS-3627G cannot be added into group even if it shows up on SIM topology list. 19. When MSTP is enabled, switch does not reply ping request. 20. Web display error under Linux OS with Firefox v2.0.0.12. 21. RIPv2 does not work properly with double VLAN function. 22. The switch cannot actually learn 1K multicast group when running L3 PIM or IGMP application. 23. When stacking master or one of the member failed in LACP environment, the clients on other devices cannot access network. 24. Power_ notification_trap does not respond correctly 25. When using SNMPwalk to get the FDB information from the switch, DGS-3600 cannot respond correct information if there are over 1K MAC under this interface.
v2.40.B19	v2.20.B38	1. All traffic will be mirrored when using ACL mirror function to mirror a specific IP at port 1. 2. When executing "reset" command on master switch under stacking topology, the slave switch will get into exception mode 3. DGS-3600 does not check the subnet mask (only check network address) when creating static routing table. 4. Even the TFTP Server IP Address does not set successfully via SNMP, the switch will still response fine to SNMP agent. 5. The telnet session will be terminated when creating and session coming from trusted hosts. 6. When both DGS-3600 and DSA-3100 are connected to each other and DGS-3600 will enter 'burn-in mode' when both devices are restarted at the same time. 7. DGS-3600 does not respond to trace route processes. 8. Under PIM-SM technology; for example, 3 switches are inter-connected, when switch 1 is suddenly rebooted, it will cause CPU high utilization on one of the switches. 9. OSPF AS external link does not correctly registered in the OSPF LSDB table when using OSPF ECMP. 10. User level privilege right is able to issue the administrator command. 11. Re-instate the missing web page for IP address settings in Administration configuration. 12. After the switch configuration was saved and rebooted, the ipif will become disable state. 13. The routing table in Web UI can only show the 1st page.

v2.20.B38	v1.00.B66	1. When login DGS-3612G via SSH, the cursor will move very slowly if using the left/right arrow key. 2. System will show fail message when typing "show config ?" command. 3. DGS-3600 doesn't correctly sent the trap "warmstart" when reboot and "coldstart" when power cycle. 4. Missing MIB file for compiling IGMP snooping "query info table" and "multicast VLAN table" 5. Wrong ACL profile ID priority, the ID with smaller ID should be matched first. 6. DGS-3600 Web UI cannot classified the IP address correctly when the address including the number "255", for example, 172.30.255.254/16 7. DGS-3600 cannot redistribute local address via OSPF correctly when the local network status changes. 8. When OSPF state is disabled, the "OSPF Router ID" in "show ospf" command incorrectly displayed as 0.0.0.0. 9. When monitoring MAC address via Web UI, user cannot enter the VLAN name more than 10 characters though we allow 32 characters when creating the VLANs. 10. DGS-3600 series will by-pass the trace route command when it's one of the hops in the path. It will makes the wrong result of trace route command. 11. DGS-3600 doesn't send ARP request when it become the VRRP master. 12. The EIGRP packets cannot pass through DGS-3600. 13. DGS-3600 can only check the first 128 static route entries correctly, though the total static route entries is 256. 14. When creating a new ipif on DGS-3600, the OSPF will stop working. 15. DGS-3600 will forward the multicast traffic to ports incorrectly which do not have multicast client joined. 16. DGS-3600 will hang-up after a random period when running in a multicast application. 17. DGS-3600 doesn't correctly forward the OSPF packet if that interface of OSPF is disabled. 18. CPU of DGS-3600 handles the ICMP packets incorrectly which make its utilization very high. 19. The default route of DGS-3600 will be lost after running a random period of time.

* D-Link tracking number is enclosed in ()

Known Issues

Firmware Version	Issues	Workaround
v2.50.B25	1. MTU setup doesn't support multicast. 2. Capability received bits 1000_full can not be display when advertised bits 1000_full is disabled 3. In stacking mode with enable PIM-SM and IGMP, CPU utilization maybe up to 100% when exceed 512 group forward.	1. No workaround solution 2. Fixed in the next official code 3. No workaround solution

	4. If RSPAN mode is TX, the monitored packets will take double tags when the packets egress form tagged destination port. 5. When RSPAN uses ACL mode, the user must configure source settings in source switch. 6. Some protocol packets such as OSPF hello packets can still be mirrored to the destination port when there is no redirected port in destination switch.	4. No workaround solution 5. No workaround solution 6. No workaround solution
v2.40.B19	1. ISM VLAN can not recognize IGMPv3 join packets 2. The switch can not record blocking entry in IP-MAC-Port binding ACL mode 3. LLDP packets length can not be more then 1500 byte 4. The switch can not learn LLDP message from STP block port 5. LLDP can not send out some triggered messages such as:Management Address,dot3_TLV,dot1_TLV	1. No workaround solution 2. Fixed in the next official code 3. Fixed in the next official code 4. No workaround solution 5. No workaround solution
V2.20.B38		
v1.00.B66	1. If the size of the config file is more then 2M, the device will lose some config. 2. Chip Limitations: ● Flow control can support "5 ports to 1 port" at best. ● For egress mirror, the target port will always receive "tagged" packets. ● "CPU interface filtering" can't filter source MAC address. 3. If the size of the next firmware is more then 4M, it can't support to upgrade to this firmware directly.	1. Fixed in the next official code 2. No workaround solution 3. Fixed in V2.50B51