



Firmware Version: V2.60.B26
Prom Code Version: V1.00.B13
Published: February 25, 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 the "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.

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 by using CLI (serial port).....	2
Upgrade by using Web-UI	3
New Features:	6
Changes in MIB & D-View Module:	10
Changes in Command Line Interface:	13
Problems Fixed:	14
Known Issues:	15
Related Documentation:	15

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
Runtime: V2.60.B26 Prom: v1.00.B13	27-July-09	DGS-3426	A1, A2
		DGS-3426P	A1, A2
		DGS-3427	A1, A2
		DGS-3450	A1, A2
Runtime: V2.35.B09	24-Oct-08	DGS-3426	A1, A2
		DGS-3426P	A1, A2
		DGS-3427	A1, A2
		DGS-3450	A1, A2
Runtime: V2.30.B10	15-Oct-07	DGS-3426	A1, A2
		DGS-3426P	A1, A2
		DGS-3427	A1, A2
		DGS-3450	A1, A2
Runtime: V2.00.B52	05-May-07	DGS-3426	A1, A2
		DGS-3426P	A1, A2
		DGS-3427	A1, A2
		DGS-3450	A1, A2
Runtime: V1.20.B23	05-June-06	DGS-3426	A1, A2
		DGS-3426P	A1, A2
		DGS-3427	A1, A2
		DGS-3450	A1, A2
Runtime: V1.00.B35	27-Jan-06	DGS-3426	A1
		DGS-3427	A1
		DGS-3450	A1

Upgrade Instructions:

D-Link switches support firmware upgrade via TFTP server. You may 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 by using CLI (serial port)

Connect a work station to the switch console port and run terminal emulation program capable of emulating 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 a user name and a password. Upon the initial connection, there is no user name 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 to the switch.
config firmware <drive_id> <pathname 64>	Change the boot up image file.

boot_up	
show boot_file	Display the file name of current boot image and configuration.
Reboot	Reboot the switch.

Example:

Switch:5# download firmware_fromTFTP 10.53.13.201 c:\ R260B23.had c:\ firm1
 Command: download firmware_fromTFTP 10.53.13.201 c:\ R260B23.had c:\ firm1

Connecting to server.....Done.

Download firmware.....Done. Do not power off!

Upload file to FLASH.....Done.

Switch:5# config firmware c:\ firm1\ R260B23.had boot_up
 Command: config firmware c:\ firm1\ R260B23.had boot_up

Success.

Switch:5# show boot_file
 Command: show boot_file

```
-----
Unit ID : 1
Boot up firmware image : C:\ R260B23.HAD
Boot up configuration file: C:\STARTUP.CFG
-----
```

Switch:5# reboot
 Command: reboot
 Are you sure you want to proceed with the system reboot? (y|n) y

Please wait, the switch is rebooting...

Upgrade 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 of workstation and enter the IP address of the switch. The system 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.
4. To update the switch's firmware or configuration file, select **Administration > TFTP Services** in function tree. Select Download Firmware in **Operation**.

5. Select the type (IPv4 or IPv6) of IP address of the TFTP server and enter the IP address.
6. Enter the firmware file name in **Local File Name**.
7. If the switch is under stacking mode, select the Unit ID of the switch upgrading the firmware.
8. Enter the path you would like to store the firmware file in **Image File In Flash**. For example C:\firm1.
9. Click **“Start”**
10. Wait until the “File Transfer” status reaches **100%** and the “Program Firmware” status shows **Completed**.

11. To select the boot up image used for next reboot, click **Administration > File System Services > System Boot Information** in the function tree.

12. Enter the complete path/file name and click **“Apply”**. For example C:\firm1\R260B23.had
13. Reboot the system.

Reboot System

If you do not save the settings, all changes made in this session will be lost.

Do you want to save the settings? Yes No

Restart

New Features:

Firmware Version	New Features
V2.60.B26	<ol style="list-style-type: none"> 1. Selective Q-in-Q <ul style="list-style-type: none"> - VLAN Translation 2. L2 Protocol Tunneling 3. LLDP 4. sFlow 5. IMPB v3.5 6. Web-based Access Control (WAC) <ul style="list-style-type: none"> - supports identity-driven QoS: Can assign ingress/egress bandwidth control and 802.1p default priority to the port according to the attributes dispatched from RADIUS server - Can enable / disable "RADIUS or Locally Assigned Information": when enabled, the Switch will accept the parameters (if applicable) assigned from RADIUS server or Local database and treat them as highest priority. 7. MAC-based Access Control (MAC) enhancement <ul style="list-style-type: none"> - supports identity-driven QoS: Can assign ingress/egress bandwidth control and 802.1p default priority to the port according to the attributes dispatched from RADIUS server - Can enable / disable "RADIUS or Locally Assigned Information": when enabled, the Switch will accept the parameters (if applicable) assigned from RADIUS server or Local database and treat them as highest priority. 8. JWAC enhancement <ul style="list-style-type: none"> - update server entries increased to 100 - supports identity-driven QoS: Can assign ingress/egress bandwidth control and 802.1p default priority to the port (port-based) or host (host-based) according to the attributes dispatched from RADIUS server - customizable page - changed the default time for JWAC quarantine server error timeout from 30 seconds to 60 seconds - increased the maximum concurrent user login to 50 per port and 100 per device - Can enable / disable "RADIUS or Locally Assigned Information": when enabled, the Switch will accept the parameters (if applicable) assigned from RADIUS server or Local database and treat them as highest priority. 9. 802.1X enhancement <ul style="list-style-type: none"> - able to force 802.1X client to go offline - supports 802.1X PDU forwarding when 802.1X is disabled - supports identity-driven QoS: Can assign ingress/egress bandwidth control and 802.1p default priority to the port according to the attributes dispatched from RADIUS server - supports maximum of 128 clients per port, 1,024 clients per switch and 4,000 clients per stack - Compatible with Cisco ACS Server: admin can use Cisco ACS RADIUS Server for 802.1X authentication - Can enable / disable "RADIUS Assigned Information": when enabled, the Switch will accept the parameters (if applicable) assigned from RADIUS

- server and treat them as highest priority.
10. Compound Authentication
 11. Authentication Database Failover: Be able to switch to local database for authentication when RADIUS server fails
 12. RADIUS Accounting: accounting and billing services for 802.1X Clients
 13. Per-flow Bandwidth Control (ACL Flow Metering)
 - CIR (Committed Information Rate)
 - Two-rate Three Color Marker (TrTCM)
 - Single-rate Three Color Marker (SrTCM)
 14. DHCP Server
 15. DHCP Server Screening
 16. RSPAN
 17. IGMP Snooping enhancement
 18. IGMPv3 Snooping: In order to comply with IGMP v3 snooping standard, change the behavior that decide IGMP packet forwarding path from checking MAC address (the behavior in V2.35.B09) to IP address (the behavior in V2.60.B26).
 - IGMP Snooping Fast Leave for IGMPv2 host
 - IGMP Snooping Report Suppression
 - IGMP Snooping dynamic group entries changed from 2K to 1K, which is shared with 64 static group entries
 - When a port receives unicast protocol packets (such as OSPF Hello packet), this port cannot change to dynamic router port; when a port receives multicast protocol packets (such as DVMRP probe, PIM Hello packet or IGMP query packets), this port will change to dynamic router port
 19. MLD Snooping enhancement
 - MLDv2 Snooping
 - MLD Snooping dynamic group entries changed from 1K to 511
 20. L2 Multicast VLAN Replication (Static configuration): Admin can manually configure the switch to route multicast traffic across VLANs
 21. STP Root Restriction (defined in 802.1Q-2005)
 22. 802.1D-2004
 23. Gratuitous ARP: Learning of Gratuitous ARP is disabled by default. This is to provide stricter security protection for the switch - to avoid attacking gratuitous ARP from the hackers. Hence it might impact the existing deployment if the connected device uses gratuitous ARP. In this case then the learning needs to be enabled
 24. Three-Level User Account
 25. ACL enhancement
 - User-defined packet content and mask
 - Flow-based (ACL) mirroring
 - ACL Statistics (counters)
 - display remaining ACL rules
 - replace_dscp action for Ethernet ACL

26. 2nd IPv4 Static Default Route
27. DHCP Relay option 60 & 61
28. Password Encryption
29. DHCP-NAP support
30. Telnet Client
31. Trusted Host enhancement
 - Can create trusted host not only for one IP but also for network range
 - Can delete all trusted hosts with one command
32. Bandwidth Control enhancement
 - changes per-port min. granularity from 64kbps to 1kbps
33. Ping MIB
34. Traceroute MIB
35. Entity MIB
36. Can enable / disable SNMP State; default is disable
37. When primary route is active, always use primary route over backup route.
38. When DHCP Relay is enabled, the Switch will block all broadcast DHCP packets in the local IP Interface
39. LBD will send traps when loops are detected and recovered
40. Configurable SSH Server TCP port
41. When configuring static multicast_fdb, typing 01005exxxxxx or 333xxxxxxx is not allowed
42. ipif_ipv6_link_local_auto can be enabled or disabled; default is disabled
43. Added parameter 'ip address' to the command "show iproute"
44. Admin can specify which Firmware image ID the switch will use during boot-up
45. Added an extra /y parameter for commands which prompt (Y/N)
46. Admin can manually configure per-port speed (capability advertisement) used for Auto Negotiation between ports: admin can configure a port to advertise a certain speed (10_full) even if it's connected to a port set to auto.
47. Network Monitoring Commands enhancement
 - "show utilization ports" will display TX/RX packets/second
 - "show error ports" will display TX/RX counters
 - "show ports" will display more details (auto negotiation / port transceiver type)
48. Enabled "Show FDB" by VID as well as by VLAN Name
49. Enabled "Show VLAN" by VID as well as by VLAN Name
50. Web-based GUI: Changed D-Link logo's link to www.dlink.com.tw
51. Attack log will include IP address, MAC address and port number
52. Admin account can remove MAC address display from log
53. "Show Fan Status" command enhanced with log and trap
54. "Show STP ports" command is standardized for all slave and master switches in a stack
55. Added MIB for "Show Memory" usage and percentage (DRAM utilization, Flash utilization)

	<p>56. Added link up/down trap per port (RFC 2233)</p> <p>57. Modified RPS MIB description and added traps</p> <p>58. OID added to show port utilization</p> <p>59. OID added to clear FDB and ARP table</p> <p>Notes:</p> <p>Please make sure all the switches in a stack are upgraded to R2.60, since some new or enhanced features might not work properly in a mixed-code stack.</p>
V2.35.B09	<ol style="list-style-type: none"> 1. MAC/Port-based MAC authentication with Switch or RADIUS 2. MAC-based VLAN 3. Cable Diagnostics 4. Loopback Detection 4.0 5. PVID auto-assignment 6. Port-based JWAC function 7. D-View 6.0 support 8. 802.1X Guest VLAN 9. New CLI Command: "show mac based vlan" 10. Serial Number Display (Web, MIB and CLI)
V2.30.B10	<ol style="list-style-type: none"> 1. JWAC support 2. ISM VLAN 3. Inter-VLAN routing enhancement <ul style="list-style-type: none"> - No need to manually configure host's MAC address
V2.00.B52	<ol style="list-style-type: none"> 1. Physical Stacking via optional CX4 (or XFP) module 2. Allows trunking or mirroring to span multiple units of the stack 3. Support per-port / per-device BPDU filtering 4. 802.1v Protocol-based VLAN 5. Double VLAN 6. Guest VLAN 7. Supports 32 IP Interfaces 8. Time-based ACL 9. IP-MAC-Port Binding (IMPB) 10. DHCP Relay Option 82 11. IPv6 Ready Logo Phase 1 12. Supports Ether-like MIB, IF MIB 13. Enhancement for broadcast storm control logging 14. Provides enhanced messages about "Current Tagged ports", "Current Untagged ports", and "Static Tagged ports" when using "show vlan" command 15. Supports "Delete ACL all" command in CLI, web and SNMP 16. Add "ping" command to user privilege 17. Adding the missing "query info table" MIB

Changes in 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>. For detailed changes of MIB content, please refer to the modification history in each MIB file.

Firmware Version	MIB File	New Features
V2.60.B26	Q-in-Q MIB	Selective Q-in-Q
	Agent-MIB	Gratuitous ARP
	LLDP-MIB	LLDP
	LLDP-dot-MIB	
	LLDP-dot3-MIB	
	SFLOW-MIB	sFlow
	DHCP-Server-MIB	DHCP Server
	AUTH-MIB	<ol style="list-style-type: none"> 1. Compound Authentication 2. 802.1X enhancement <ul style="list-style-type: none"> - able to force 802.1X client to go offline - supports 802.1X PDU forwarding when 802.1X is disabled - supports identity-driven QoS: Can assign ingress/egress bandwidth control and 802.1p default priority to the port according to the attributes dispatched from RADIUS server. - supports maximum of 128 clients per port, 1,024 clients per switch and 4,000 clients per stack 3. Can enable / disable "RADIUS or Locally Assigned Information": when enabled, the Switch will accept the parameters (if applicable) assigned from RADIUS server or Local database and treat them as highest priority
	RSPAN-MGMT-MIB	RSPAN
	RADIUS-ACCOUNTING-MIB	RADIUS Accounting
	FILTER-MIB	DHCP Server Screening
ACLMGMT-MIB	<ol style="list-style-type: none"> 1. Per-flow Bandwidth Control (ACL Flow Metering) <ul style="list-style-type: none"> - CIR (Committed Information Rate) - Two-rate Three Color Marker (TrTCM) - Single-rate Three Color Marker (SrTCM) 2. ACL enhancement <ul style="list-style-type: none"> - User-defined packet content and mask - Flow-based (ACL) mirroring - ACL Statistics (counters) 	

	<ul style="list-style-type: none"> - display remaining ACL rules - replace_dscp action for Ethernet ACL
IP-MCST-VLAN-REP-MIB	L2 Multicast VLAN Replication (Static configuration): Admin can manually configure the switch to route multicast traffic across VLANs
MSTP-MIB	STP Root Restriction (defined in 802.1Q-2005)
MLD-SNOOPING-MIB	MLD Snooping enhancement <ul style="list-style-type: none"> - MLDv2 Snooping
IP-MAC-BIND-MIB	IMPB v3.5
JWAC-MIB	JWAC enhancement <ul style="list-style-type: none"> - update server entries increased to 100 - customized page - changed the default time for JWAC quarantine server error timeout from 30 seconds to 60 seconds - increased the maximum concurrent user login to 50 per port and 100 per device
WebBase-Access-Control-MIB	Web-based Access Control (WAC) <ul style="list-style-type: none"> - supports identity-driven QoS: Can assign ingress/egress bandwidth control and 802.1p default priority to the port according to the attributes dispatched from RADIUS server.
Mac-based-Authentication-MIB	MAC-based Access Control (MAC) enhancement <ul style="list-style-type: none"> - supports identity-driven QoS: Can assign ingress/egress bandwidth control and 802.1p default priority to the port according to the attributes dispatched from RADIUS server.
SSH-MIB	Configurable SSH server TCP port
DGS-3426-L2MGMT-MIB DGS-3426P-L2MGMT-MIB DGS-3427-L2MGMT-MIB DGS-3450-L2MGMT-MIB	<ol style="list-style-type: none"> 1. IGMP Snooping enhancement <ul style="list-style-type: none"> - IGMPv3 Snooping - IGMP Snooping Fast Leave for IGMPv2 host - IGMP Snooping Report Suppression 2. LBD will send traps when loops are detected and recovered 3. Bandwidth Control: min. port granularity changed from 64kbps to 1kbps 4. Admin can manually configure per-port speed advertisement: used for Auto Negotiation between ports
DGS-3426-L3MGMT-MIB DGS-3426P-L3MGMT-MIB DGS-3427-L3MGMT-MIB DGS-3450-L3MGMT-MIB	<ol style="list-style-type: none"> 1. DHCP Relay option 60 & 61 2. 2nd IPv4 Static Default Route 2. ipif_ipv6_link_local_auto can be enabled/disabled; disabled by default
AGENT-GENERAL-MIB	<ol style="list-style-type: none"> 1. Trusted Host enhancement

		<ul style="list-style-type: none"> - Can create trusted host not only for one IP but also for network range - Can delete all trusted host with one command <ol style="list-style-type: none"> 2. Admin can specify which Firmware image ID the switch will use during boot-u 3. MIB for Show Memory usage and percentage 4. OID to show port utilization 5. OID to clear FDB and ARP table
	EQUIPMENT-MIB	<ol style="list-style-type: none"> 1. Enable logs and traps for Show Fan Status 2. Modified RPS MIB description and added traps
	IF-MIB	Link up/down trap per port (RFC 2233)
	DISMAN-PING-MIB	Ping MIB
	DISMAN-TRACEROUTE-MIB	Traceroute MIB
	ENTITY-MIB	Entity MIB

Changes in 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.

Firmware Version	Changes
V2.60.B26	None

Problems Fixed:

Firmware Version	Problems Fixed
V2.60.B26	<ol style="list-style-type: none"> When DGS-3400s are in stacking mode, powering off unit 1~5 and then powering them back will sometimes cause stack recovery failure. (DI20080818000001) After user resets the switch and then enables stacking via Web GUI, the switch cannot be pinged. (DI20081224000007) Web GUI does not display ACL rules correctly. (DI20090618000010) Admin cannot use the CLI command "config double_vlan d169 add access 23" to add double VLAN access member port. (DT20081222000002) SSH Login: When using OpenSSH 5.1p1 and a particular script file to test, the switch will enter exception mode. (DI20081106000011) Loopback Detection (LBD) will not always activate if the loop traffic includes STP BPDU. (DI20081118000011)
V2.35B09	<ol style="list-style-type: none"> Sometimes Link Aggregation group does not function when stacking mode is enabled Under certain setup the desired VLAN is not being assigned to authenticated wireless client but instead the AP's managed VLAN In stacking mode, sometimes backup master will not become master when the master fails in a stack Remove the PoE menu from Web GUI for non-PoE DGS-3400 models
V2.30B10	<ol style="list-style-type: none"> Single IP Management (SIM) only works with default VLAN Password string display disclosed when the first character has been removed Instability issue between Intel 10G NIC and DGS-3400 Series 10G modules (DEM-410CX) which causes link down/link up frequently
V2.00B52	<ol style="list-style-type: none"> User logins in through SSH successfully but log shows that both SSH login and console login event happen at the same time Switch hangs when using Telnet to create 128 ACL rules Wrong ACL OID is retrieved via snmpwalk tool Syslog cannot accurately classify the severity of the message Switch enters Exception Mode when saving through Telnet Creating ACL via Web GUI will cause the web management to go down Creating CPU filtering ACL will cause the web management to go down SNMP compatibility issue at ACL with Firewall DFL-1600 Wrong warm_start trap type is sent while rebooting DGS-3400 series cannot use web to check MAC address table by using vlan name if the vlan name is longer than 10 digits
V1.20B23	<ol style="list-style-type: none"> Modify the naming of "LoopBack Guard" to "Loopback Detection" on Web GUI Change the default IP address to "10.90.90.90/8"
V1.00B35	Initial Release

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues	Workaround
V2.60.B26	<p>DGS-3450 only: Per port mapping of 802.1p priority and class is not supported when packets flowing between block 1 (port 1~24) and block 2 (port 25~48), and across devices in the same physical stack. When this happens the switch will use default mapping instead of the configured class mapping</p>	None

Related Documentation:

- DGS-3400 Series User Manual
- DGS-3400 Series CLI Manual