Firmware Version: v2.00.016
Prom Code Version: v1.00.016
Published: 2011/08/08

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

1. 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.
2. 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.
3. 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:

Firmware Version	Date	Model	Hardware Version
Runtime: v2.00.016 Prom: v1.00.016	2011/08/08	DGS-3200-24	A1
		DGS-3200-16	A1, A2
		DGS-3200-10	A1, A2, A3, B1
Runtime: v1.50.B052 Prom: v1.00.B013	2010/10/06	DGS-3200-24	A1
		DGS-3200-16	A1, A2
		DGS-3200-10	A1, A2, A3, B1
Runtime: v1.50.B019 Prom: v1.00.B012	2009/10/01	DGS-3200-24	A1
		DGS-3200-16	A1, A2
		DGS-3200-10	A1, A2, A3, B1
Runtime: v1.35.B023 Prom: v1.00.B006	2009/03/20	DGS-3200-16	A1, A2
		DGS-3200-10	A1, A2, A3
Runtime: v1.11.B004 Prom: v1.00.B005	2008/09/10	DGS-3200-16	A1
		DGS-3200-10	A1, A2
Runtime: v1.11.B003 Prom: v1.00.B005	2008/05/29	DGS-3200-16	A1
		DGS-3200-10	A1
Runtime: v1.00.B015 Prom: v1.00.B004	2007/10/30	DGS-3200-10	A1

Upgrade Instructions:

* It is not necessary to upgrade PROM code.

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 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 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> | <ipv6addr>] <path_filename 64> image_id <1-2>]	Download firmware file to the switch.
config firmware image_id <1-2> [delete | boot_up]	Change the boot up image file.
show firmware information	Display the file name of current boot image and configuration.
reboot	Reboot the switch.

Example:

1. **DGS-3200-10:4#download firmware_fromTFTP 10.90.90.91 DGS3200_Run_1_35_B023.had image_id 1**

```
 Command: download firmware_fromTFTP 10.90.90.91 DGS3200_Run_1_35_B023.had
 image_id 1

Connecting to server................... Done.
Download firmware...................... Done.  Do not power off!
Please wait, programming flash......... Done.
```

2. **DGS-3200-10:4#config firmware image_id 1 boot_up**

```
 Command: config firmware image_id 1 boot_up

Success.
```

3. **DGS-3200-10:4#show firmware information**

```
 Command: show firmware information

Image ID      : 1(Boot up firmware)
Version       : 1.35.B023
Size          : 2206933 Bytes
Update Time   : 2009/03/20 14:11:43
From          : 10.90.90.91(Console)
User          : Anonymous

Image ID      : 2
Version       : 1.11.B004
Size          : 2099223 Bytes
Update Time   : 0 days 00:00:00
From          : Serial Port(Prom)
User          : Unknown
```

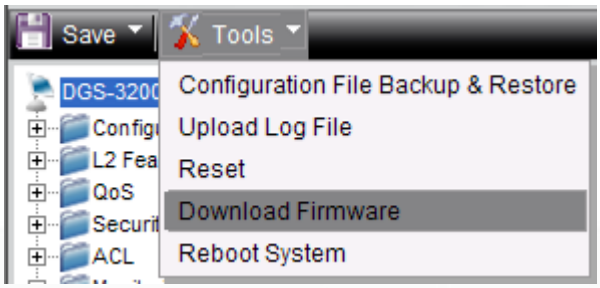
4. **DGS-3200-10:4#reboot**

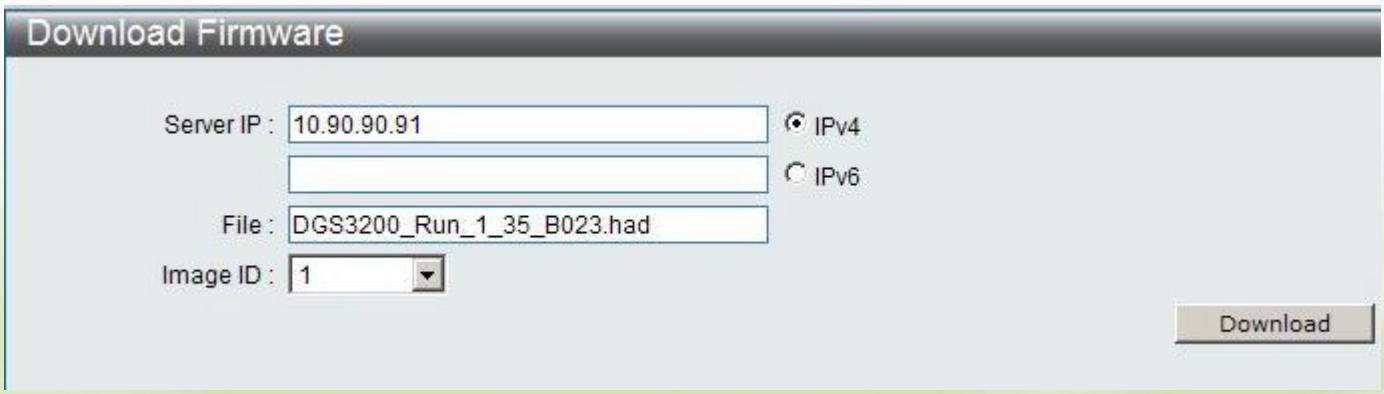
```
 Command: reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

```
Boot Procedure                                                  V1.00.B006
-------------------------------------------------------------------------------

Power On Self Test ....................................  100%

MAC Address   : 00-00-01-02-03-04
H/W Version   : A2

Please Wait, Loading V1.35.B023 Runtime Image .............  100%


Device Discovery .....................................  100 %
Configuration init ...................................  100 %


                DGS-3200-10 Gigabit Ethernet Switch
                     Command Line Interface

                   Firmware: Build 1.35.B023
      Copyright(C) 2009 D-Link Corporation. All rights reserved.
UserName:
```

Upgrade by using Web-UI

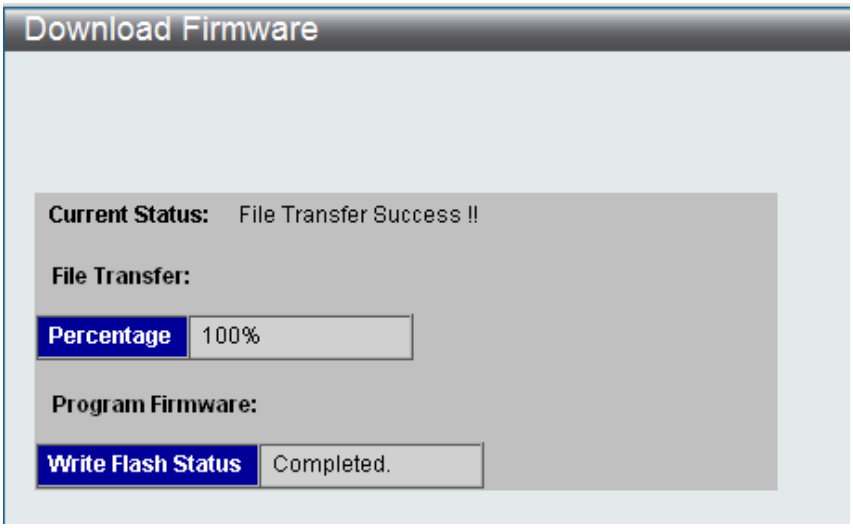
1. Connect a workstation installed with java SE runtime environment to any switch port of the device.
2. Open the web browser from the workstation and enter the IP address of the switch. The switch's default IP address is 10.90.90.90.
3. Enter administrator's username and password when prompted. It should be noted that the username and password are blank by default.
4. To update switch's firmware or configuration file, select ***Tools > Download Firmware*** from the banner.





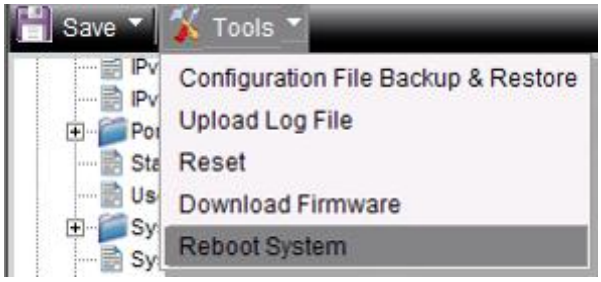
5. Select the type (IPv4 or IPv6) of IP address of the TFTP server and enter the IP address.

6. Enter the name of the firmware file located on the TFTP server.
7. Select the Image ID you would like to store the firmware file.
8. Click "***Download***" button.
9. Wait until the "File Transfer" status reaches 100% and the "Program Firmware" status shows "completed".

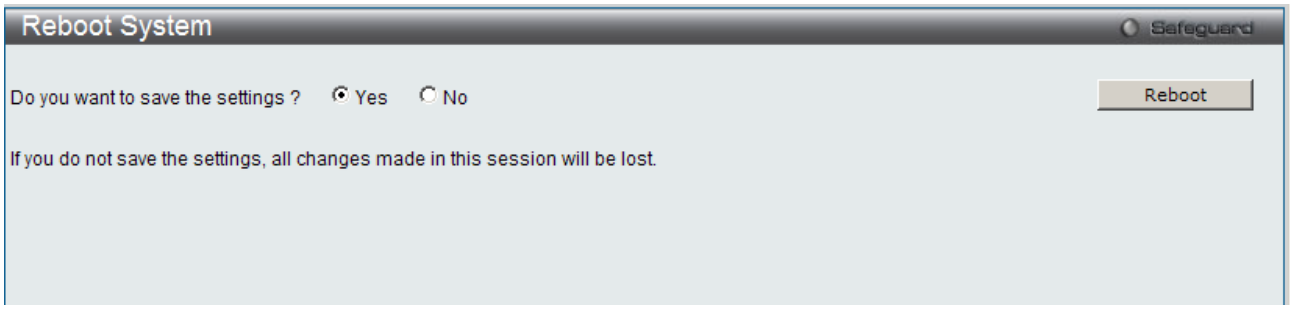


10. To select the boot up image used for next reboot, click ***Configuration > Firmware information*** in the function tree. Click corresponding "***Set Boot***" button to specify the firmware that will be used for next and subsequent boot up.

11. To reboot the switch, select ***Tools > Reboot System*** from the banner.



12. Select "***Yes***" and click "***Reboot***" button to reboot the switch.



New Features:

Firmware Version	New Features
V2.00.016	1. Enhance trusted host to support 30 entries and by application 2. Support DHCPv6 client 3. DHCPv6 Snooping + NDP Snooping + IMPBv6 4. Change parameters "countdown" to "3-30" minutes and "time_interval" to "5 - 600" seconds in broadcast storm control. 5. Support IEEE 802.3ah 6. Host-based IGMP snooping fast leave 7. Enlarge password length to 32 characters for user account 8. Enhance Greeting Message to support 24 lines, each line supports 80 bytes 9. Support get memory status via SNMP 10. Authentication Database Failover enhancement: Add a parameter that when radius server times out, bypass client authentication 11. Add DHCP local relay option 82 with keep, replace and drop action 12. DHCP option 12 13. Add a MIB file to get switch's serial number 14. Support to disable a trunk member port 15. Configurable CLI terminal length 16. Support static IGMP snooping group 17. Support exception/debug handler, if there is an exception happens, the switch will save all necessary information into flash then reboot the switch automatically. After that, user can download the debug information by TFTP process. 18. IMPB v3.82 19. Enhance show config command to see specific effective and modify parts.

20. Change max. 802.1X host-based access control user from per port limitation to share per system pool basis.
21. Support edge port in STP mode
22. Support Command logging with account message
23. JWAC monitor enhancement (show IP address and user ID with MAC address for authenticated JWAC user)
24. Support PPPOE circuit ID insertion
25. ''Show fdb security' command to show MAC entries created by security modules
26. Radius accounting for WAC
27. Send a trap after save, download/upload configuration file completed
28. Send a trap when upgrade firmware via SNMP is finish
29. Support NLB
30. Support BPDU Attack Protection
31. Support LLDP-MED
32. Support config max_mcast_group with replace and drop action when exceed max multicast group
33. Support FQDN: DNS Resolver
34. Disable the " refresh " behavior when the clipaging is disabled.
35. Log enhancement: Spoofing attack to include IP address along with mac address and port number
36. Support Voice VLAN v2.1
37. ACL assignment after successful authentication
38. Support filter command under show config current_config, NVRAM and upload_config
39. Changing the way to configure port speed and duplex settings
40. Enhancement of "show ports" command by adding extra information, eg. media type, speed, utilization and etc….
41. Provide flexibility to alter/change the default port no. of SSH from 22 to the desire port.
42. Add a MIB to create static FDB
43. Support DHCPv6 Relay Agent
44. Support "show error ports" command
45. Auto-recovery for disabled ports from broadcast storm control
46. Support intermediate CA Certificate
47. Support JWAC roaming
48. Support LACP trap definition v1.1
49. Support pre-config TFTP setting
50. Support 802.3ah extension – DULD
51. Support "show tech support" troubleshooting command
52. Rename "Multiple Authentication" to "Compound Authentication"
53. When typing 'show config' command, show encrypted password in "enable admin" section
54. Support Gratuitous ARP
55. Support per queue bandwidth control
56. Pass through reserved multicast packet when enabling igmp_snooping or

	configuring filter_unregistered_group 57. Add new MIB definition for DLINK Zone Defense 58. Sending Acct-Status-Type=Start when joining igmp group 59. Support MAC Blackhole 60. Support SD card management 61. Add force_agree parameter to immediately execute the reboot/reset command without further confirmation. 62. Support Loopback detection v4.03 63. Support Password recovery enable/disable 64. Support WAC customize web page 65. Support user privilege authorization by TACACS+ authentication 66. Support RADIUS VLAN assignment with VLAN ID or VLAN name by different tag 67. Support option82 remote-ID user-configurable or option82 removable option when DHCP Local Relay enabled 68. L2 protocol Tunneling (L2PT) 69. Support configuration file can be config with filename 70. D-Link Green 3.0 4. Power Saving by LED Shut-Off 5. Power Saving by Port Shut-Off 6. Power Saving by System Hibernation 71. Support DHCP Server 72. Open user level access right to Cable Diagnostics feature
V1.50.B052	None
v1.50.B019	1. Support new model DGS-3200-24. 2. Support Private VLAN feature. 3. Authentication database failover: Be able to switch to local database for authentication when RADIUS server fails. 4. Support the allocation of configuration and image files into the SD memory card on the front panel. 5. L3 Control Packet Filtering: Support the filtering of DVMRP, PIM, IGMP Query, OSPF, RIP, or VRRP packets. 6. ACL Counter feature that shows the ACL usage statistics. 7. Support the display of system uptime in CLI. 8. Support ARP Snooping Prevention that provides an alternative to 'IMPB', with simpler configuration (only check IP/MAC binding). 9. Enhance the support of max trunk groups for DGS-3200-10 to 5 groups, DGS-3200-16 to 8 groups and DGS-3200-24 to 12 groups. 10. D-Link green technology: Support cable length detection for power saving. 11. Support ACL wizard feature in WEB interface. 12. IP-MAC-Port Binding (IMPB) v3.61. ● Configurable threshold number for illegitimate entries that can be recorded in the FDB (IMPB v3.5) ● Prevent legitimate user from launching unicast ARP spoofing attacks.(IMPB v3.61)

	13. SNMP trap support for SIM, STP and MAC-based access control. 14. Accept RADUIS VLAN assignment with VLAN name and type formats. So it can comply with Cisco RADIUS Server. 15. Support the configuration of 31bit subnet-mask prefix(RFC3021) 16. Support SNMP traps for the link status change. 17. Add show reports and router port in IGMP Snooping group 18. For DGS-3200-24 only: Add an OID 1.3.6.1.4.1.171.12.11.1.8.1 to detect temperature 19. For DGS-3200-24 only: Supports per-port MAC for the protocol packets including GVRP, STP, 802.1X, CTP and LACP 20. For DGS-3200-24 only: Support File system for SD card
v1.35.B023	1. D-Link green technology: Support link status detection for power saving. 2. Support IPv6 ready logo core phase II certification. 3. Multiple Authentication. 4. DHCP Server Screening. 5. VLAN trunking. 6. IGMP authentication. 7. ISM VLAN. 8. Cable diagnostics. 9. IP-MAC-Port Binding v3.4 10. Web-based access control v2.0 7. RADIUS to Local database failover 8. HTTPs 9. Detailed ports auth_state 11. IGMP Snooping enhancement: Data Driven Learning so the switch will build up the entry in its multicast table when sniffing the multicast traffic from the media server. Typically used in an environment where the multicast server is connected to the switch directly. 12. LBDv4.0 trap. 13. Enlarge port security to 64 entries. 14. Add “UP Time and Expiry Time” column while “show igmp_snooping group”. 15. Support DHCP local relay to insert option 82 information on DHCP broadcast packets in client’s VLAN. 16. Block broadcast packet in DHCP relay. 17. Egress filter to drop all unknown unicast/multicast packets. 18. Customize JWAC authentication welcome page. 19. MAC-based access control can be dynamic VLAN assignment without Guest VLAN enabled. 20. Display replying IP instead of broadcast IP for ping broadcast address. 21. Enhance port-based bandwidth control granularity from 512Kb/s to 64kb/s. 22. Enhance MAC-based Access Control for the authentication process which initiated by capturing "new traffic" which instead of "ARP or DHCP” packet. 23. Add an OID 1.3.6.1.4.1.171.12.11.1.8 to detect temperature (only supported on DGS-3200-16)

v1.11.B004	1. Support DGS-3200-10 A2 hardware
v1.11.B003	1. Support new model DGS-3200-16 2. Upgrade PROM code via TFTP 3. Product serial number can be displayed on GUI, CLI and be queried via SNMP 4. Fan failure and recovery logs/trap 5. Capability to display the fan status (only for DGS-3200-16) 6. Add port information on STP log event while STP topology changes 7. 802.1v protocol VLAN 8. ACL/CoS user defined packet content 9. RADIUS accounting for JWAC 10. Add mask function on trusted host 11. IPv6 Microsoft NAP supported 12. Support IPv6 RADIUS authentication 13. Enable logout feature and logout timer for WAC 14. TFTPv6 client 15. RMON v2 (Probe config group) 16. IPv6 management via WEB, SNMP, Telnet 17. ICMPv6 18. IPv6 Neighbor Discovery 19. IGMP v3 snooping 20. Support 24 multicast filter profiles and 128 limited IP multicast address ranges per profile 21. Static MAC-based VLAN 22. Support JWAC target VLAN mode 23. Add Ping & TRACEROUTE MIB 24. Add the ability to forward the unregistered multicast traffic to router port even when the 'filter unregistered groups' option is enabled
v1.00.B015	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. For detailed changes of MIB content, please refer to the modification history in each MIB file.

Firmware Version	MIB File	New Features
V2.00.016	Auth.mib	Authentication Database Failover enhancement: Add a parameter that when radius server times out, bypass client authentication
	BPDUProtection.mib	BPDU Attack Protection
	DNSResolver.MIB	FQDN: DNS Resolver

	DHCPv6Relay.mib	DHCPv6 Relay Agent
	DHCPServer.mib	DHCP Server
	DULD.mib	IEEE 802.3ah extension – DULD
	Equipment.mib	D-Link Green v3.0
	Genmgmt.mib	1. Enhance trusted host to support 30 entries and by application 2. Get memory status via SNMP 3. Command logging with account message 4. Send a trap after save, download/upload configuration file completed 5. Send a trap when upgrade firmware via SNMP is finish 6. Gratuitous ARP
	IPMacBind.mib	1. IMPBv3.82 2. DHCPv6 Snooping + NDP Snooping + IMPBv6
	Jwac.mib	1. JWAC monitor enhancement (show IP address and user ID with MAC address for authenticated JWAC user) 2. JWAC roaming
	l2mgmtDGS3200.mib l2mgmtDGS3216.mib l2mgmtDGS3224.mib	D-Link Green 3.0
	L2ProtocolTunnel.mib	L2 protocol Tunneling (L2PT)
	McastFilter.mib McastVLAN.mib McastSnooping.mib	1. Support config max_mcast_group with replace and drop action when exceed max multicast group 2. Pass through reserved multicast packet when enabling igmp_snooping or configuring filter_unregistered_group
	NLB.mib	NLB
	PktStormCtrl.mib	1. Change parameters "countdown" to "3-30" minutes and "time_interval" to "5 - 600" seconds in broadcast storm control. 2. Auto-recovery for disabled ports from broadcast storm control
	PPPoEmgmt.mib	PPPOE circuit ID insertion
	radiusAccounting.mib	Radius accounting for WAC
	SSL.mib	Intermediate CA Certificate
	StaticFDB.mib	Add a MIB to create static FDB
	SDCardMgmt.mib	SD card management
	wac.mib	WAC customize web page

	VoiceVLAN.mib	Voice VLAN v2.1
	ZoneDefense.mib	New MIB definition for DLINK Zone Defense
	lldp.mib lldp-dot1.mib lldp-dot3.mib lldp-med.mib	LLDP-MED
	Standard MIB: IPV6-TC.mib DIFFSERV-DSCP-TC.mib ianaaddressfamilynumbers-mib.mib IEEE8023-LAG-MIB.mib rfc2856(HCNUM_TC).mib rfc4836(MAU).mib IANA-MAU-MIB.mib ie8023ah.mib INET-ADDRESS-MIB.mib	
V1.50.B052	No new update	None
v1.50.B019	PrivateVLAN.mib	Private VLAN
	Auth.mib mba.mib Wac.mib Jwac.mib	Authentication database failover
	Filter.mib	L3 Control Packet Filtering
	ACL.mib	ACL Counter
	FS.mib	File System with SD card (DGS-3200-24
	Genmgmt.mib	File System with SD card (DGS-3200-24 only)
	RFC1213.mib	Display of system uptime in CLI
	ARPSpoofingPrevention.mib	ARP Spoofing Prevention
	Equipment.mib	1. Cable length detection 2. Add an OID 1.3.6.1.4.1.171.12.11.1.8.1 to detect temperature (DGS-3200-24 only)
	Singleip.mib	1. Support SNMP trap support for SIM, STP and MAC-based access control. 2. Support the SNMP traps for the link status change.
	IPMacBind.mib	IP-MAC-Port Binding (IMPB) v3.61
	l2mgmtDGS3200.mib l2mgmtDGS3216.mib l2mgmtDGS3224.mib	Add show reports and router port in IGMP Snooping group
v1.35.B023	RFC2925p.mib	Display replying IP instead of broadcast IP for ping broadcast address.

	CableDiag.mib	Cable diagnostics.
	Equipment.mib	1. D-Link green technology: Support link status detection for power saving. 2. Add an OID 1.3.6.1.4.1.171.12.11.1.8 to detect temperature (only supported on DGS-3200-16)
	l2mgmtDGS3200.mib, l2mgmtDGS3216.mib	1. Support DHCP local relay to insert option 82 information on DHCP broadcast packets in client's VLAN. 2. Block broadcast packet in DHCP relay. 3. Add "UP Time and Expiry Time" column while "show igmp_snooping group". 4. Data driven multicast 5. LBDv4.0 trap. 6. VLAN trunking. 7. IGMP authentication 8. Enlarge port security to 64 entries.
	Auth.mib	Multiple authentication.
	L3mgmtDGS3200.mib, L3mgmtDGS3216.mib	Support IPv6 ready logo core phase II certification.
	IPMacBind.mib	IP-MAC-Port Binding v3.4
	Filter.mib	1. DHCP server screening. 2. Egress filter to drop all unknown unicast/multicast packets.
	Jwac.mib	Customize JWAC authentication welcome page.
	wac.mib	Web-based access control v2.0 3. RADIUS to Local database failover 4. HTTPs 5. Detailed ports auth_state
	mba.mib, staticMacBasedVlan.mib	MAC-based access control can be dynamic VLAN assignment without Guest VLAN enabled.
	ISM.mib	ISM VLAN.
	RFC4188.mib	Definitions of Managed Objects for Bridges
	RFC1493.mib	Remove and obsolete by RFC4188.mib
v1.11.B004	None	
v1.11.B003	None	
v1.00.B015	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	Changes
V2.00.016	1. Remove 802.1X CLI direction control parameter 2. Username "enable" cannot be created
V1.50.B52	None
V1.50.B019	None
V1.35.B023	1. Remove config IPv6 nd rs ipif <ipif_name 12> state [enable | disable] 2. Remove config wac vlan <vlan_name 32>
V1.11.B004	None
V1.11.B003	None
v1.00.B015	First release

Problem Fixed:

Firmware Version	Problems Fixed
V2.00.016	1. When IP-MAC entry violation happens, device does not send IMPB traps. (DGC20100506000002) 2. Correct LBD function behavior for combo ports (DI20100609000006) 3. When download firmware to 21 devices which joined a SIM group at the same time, all members could not complete the firmware file transfer. (DI20100602000004) 4. If STP on SIM commander switch is enabled, upgrade firmware to all member switches will cause STP convergence re-started. (DI20100722000009) 5. Trendnet RG router TEW-633GR as a DHCP client can receive address via DHCP correctly but switch does not create associated IMPB entry by DHCP_snooping. (DRU20100708000002) 6. When connect/disconnect a LACP member port (not all member ports), STP topology change was occurred, and the traffic through the LAG port was dropped. (DI20100910000006) 7. DGS-3200 ACL cannot deny IPv6 (Ethernet type 0x86dd) packets. (DRU20101021000001) 8. The message will be displayed "Error: already register!! /dump authentication admin_user" when rebooting. (DI20101122000002) 9. When STP is enabled and traffic control for multicast (threshold 512) is set, switch receives "topology change" events, but physical links are not disconnected. (DRU20101227000003) 10. Device System IP interface cannot be ping from LACP link. (DRU20110301000004) 11. Android device cannot do JWAC authentication via RADIUS.

	(DI20110303000004) 12. After download the config via telnet, and type "save" command from console, switch will go to exception mode.(DRU20110325000008)
V1.50.B052	1. Fixed that the Private VLAN setting "promiscuous port" in Web UI is incorrectly displayed in "trunk port" part. (DI20090820000002) 2. Fixed that if DGS-3200 and PC are in different subnets (i.e., L3 switch in between), PC can receive the SNMP trap, but need to wait about 20 seconds. (DI20090820000016) 3. Fixed that after power cycle, DGS-3200 cannot receive the "cold-start" and first "linkup" trap.(DI20090820000016) 4. Fixed that under JWAC customize page, some Japanese characters, for example "入口", will fail to display correctly when save/reboot the switch. (DI20090921000002) 5. Fixed that the SD card command, drive_id cannot be specified by using tab after 'copy' or 'erase' command. (DI20090918000005) 6. Fixed that 1G SD card cannot be accessed after format by WinXP FAT16. (DI20090918000011) 7. Fixed that DGS-3200 does not send the linkchange_traps of link aggregation's member ports. (DI20090924000022) 8. Fixed that incorrect command spelling: Correct "mutlticast_vlan" to "multicast_vlan" in delete igmp_snooping mutlticast_vlan command. (DI20091001000006) 9. Fixed that DoS vulnerability in the TCP-induced: After DoS attack stops, the TCP sessions always stays in "finWait1" and doesn't time-out. (DI20090909000007) 10. Fixed that PHY enabled copper ports LED by default. Even only fiber port is connected, the PHY remains power down/up and flash one time on copper port then disappear. 11. Fixed that LBD (Loopback detect) does not work if the port is MAC-based access control enable port. (DI20091026000009) 12. Fixed that when igmp_snooping is enabled, if DGS-3200 receives one OSPF hello packet, it will send duplicated (two) such packets out. (DI20091105000011) 13. Fixed that MAC address authenticated by MAC-based access control may not be correctly displayed by CLI/telnet. (DI20091105000026) 14. Fixed that DGS-3200s' configuration file cannot be loaded completely and enters in greeting_message editor. (DI20091111000008) 15. Fixed that after correctly created LAG (Link aggregation) groups, then user creates IMPB entry in LAG ports. The LAG member port configuration cannot be loaded successfully after reboot, causing by LAG ports cannot be established. (IMPB and LAG cannot be configured at same port. If users try to configure IMPB on link aggregation port, the error message will be displayed to indicate such configuration is not allowed). 16. Fixed that incorrect value of SNMP ifNumber. (DI20091127000010) 17. Fixed that if "IMBP" and "traffic_segmentation" are enabled in DGS-3200, clients in traffic segmentation ports can receive ARP packets and DHCP broadcast packets from other clients. (DI20091203000005) 18. Fixed that DGS-3200's CPU utilization became 100% when JWAC works via

Radius. (DI20091208000004)

19. Fixed that DGS-3200 does not erase unauthenticated MAC address entry on its FDB, even after aging time out. (DI20091225000010)
20. Fixed that DGS-3200 does not erase igmp_snooping entry on LAG port when receiving IGMP v2 leave report. (DI20091225000008)
21. Fixed that MAC-based access control entry cannot erased by ageing timeout. (DI20100106000009)
22. Fixed that the incorrect display of mirror parts while “show Config”. (DI20091218000007)
23. Fixed that guest VLAN PVID was changed if changing other port’s VLAN setting. (DI20100122000010)
24. Fixed that if LAG (Link Aggregation) is configured, DGS-3200 did not transmit packets for a while when saving configuration. (DI20100122000015)
25. Fixed that when Jumbo Frame function is enabled, even PC supports Jumbo frame, PC cannot ping device after device reboot. (DEUR20100112000005)
26. Fixed that after running for a while, DGS-3200 does not send any RADIUS packets, and the ports cannot learn FDB entry when the port is enabled MAC-based access control. (DI20100128000008)
27. Fixed that DGS-3200 delete VLAN via Web UI failed, although message shows success. (DI20100204000017)
28. Fixed that two PCs supporting VLAN tagging and connected to same VLAN ID tagged port cannot communicate (e.g. ping) each other in DGS-3200 vlan_trunk enabled ports. (DI20100203000010)
29. Fixed that "tagged_only" parameter on STP port doesn't work correctly. (DI20100202000017)
30. Fixed that DGS-3200’s "arp_soofing_prevention" configured "port" has different behavior from other model. (DI20100205000009)
31. Fixed that in DGS-3200’s Web UI, user cannot edit VLAN if there is a static FDB has been created on that VLAN. (DI20100301000010)
32. Fixed that DGS-3200 does not save VLAN settings if VLAN trunking is used. (DI20100302000018)
33. Fixed that the configuration of JWAC auth_failover cannot be saved. It lost after reboot the switch. (DI20100315000006)
34. Fixed that "enable WAC function" does not saved after reboot. (DI20100317000003)
35. Fixed that when MAC-based access control and STP functions are enabled on the same port, BPDU was blocked and dropped by MAC-based access control function. STP does not work on the port and traffic storm is occurred. (DI20100422000003)
36. Fixed that Safeguard engine cannot be disabled. (DRU20100527000001)
37. Fixed that it needs to create an account "enable" onto TACACS+ server database with new password. (DRU20100602000001)
38. Fixed that DGS-3200 TFTP UDP 69 port is opened by default, even though the associated used function SIM is disabled. (DUSA20100617000001)
39. Fixed that if two or more DGS-3200 are cascaded and DHCP relay are enabled in all DGS-3200, DHCP client (DGS-3200) in down linked unit cannot obtain the IP address from DHCP server. (DRU20100707000004)

V1.50.B019	1. Client could still access the network when the configured JWAC idle timeout is reached. JWAC will now correctly age out the client after the configured idle time expires.(DI20090406000008) 2. After a client connected to DGS-3200 successfully passes 802.1X NAP authentication, an error log (event ID 6275) appears in the NPS server. A 802.1X Accounting attribute "NAS-Port-Type (61): Ethernet (15)" has been added to fix this problem. (DI20090325000019)
v1.35.B023	1. VLAN advertisement packet will not be sent if GVRP is not enabled on the client ports. (DI20080411000016) 2. Multicast groups entries are not deleted while the switch is in non-querier state and enable fast leave. (DI20080527000009) 3. The switch will not forward the group specific query to the client ports while client sends a IGMP leave message to querier switch. (DI20080521000019) 4. There will be packets loss if the switch receives massive amount of IGMPv3 reports to join the same multicast group address. (DI20080514000007) 5. Fixed the performance issue while show current_config by using telnet and SSH. (DI20080625000018) 6. When data-driven multicast is enabled if client join/leave multicast groups repeatedly, unknown multicast group will not be forwarded to router port. (DI20080627000014) 7. In 802.1X host-based access control, after a client successfully authenticates, moves to another port then move back which the ports cascaded by hub. There will be no authentication even the authentication status is "authenticated". (DI20080626000014) 8. The querier switch does not send IGMPv3 membership query message, therefore, multicast group will timeout by default 260 seconds. (DI20080707000023) 9. If serial number is not burned in the flash but the firmware supports the display of "serial number" on the switch, it will be displayed as scrambled code. Fixed the problem that there will be no serial number column if the switch doesn't burn-in serial number.(DUSA20080709000001) 10. While enable MAC-based Access Control by local database, one client connects to a port with a downlink unmanaged switch, another client connects to the switch directly, only latest client who authenticated success will pass.(DI20080813000012) 11. Incorrect authenticating state in MAC-based access control of web-GUI even no user is authenticating on that port. (DI20080818000011) 12. An incorrect message will pop up if user deletes IGMP snooping groups VID 1. (DI20081014000019) 13. While enable RSTP and LACP application, the convergence will take around 3 minutes. (DI20081104000004) 14. The "new line" symbol (0D0A) is inconsistent in configuration file. (DI20081105000024) 15. "Save all" configuration page cannot display in Firefox 3 browser on FreeBSD7.1 OS. (DI20081105000023) 16. The switch will enter exception mode while using openSSH5.1 to logon the switch. (DI20081105000022) 17. CPU utilization will go up to 100% if multiple users login via SSH. (DUSA20081105000001)

	18. While enable RSTP, SA of BPDU is always system MAC, the duplicate MAC cannot be learned on different ports and cause system IPIF no reply. (DI20081017000005)
v1.35.B023	1. While auto configuration is enabled, if DHCP server and TFTP server are in the same server, download configure will fail. (DI20081120000010) 2. There are two local3 facility parameters of syslog setting in web-GUI, which should be local4 facility. (DI20081208000009) 3. All ports will become discarding designated status when MSTP is enabled. (DI20081205000009) 4. "config scheduling 7" does not appear in configuration file. (DI20090123000006) 5. When MAC-based access control is enabled on port1, client can pass authentication, however, if the same client moves to port 8, which does not have MAC-based access control enabled, client will be blocked. (DI20090114000016)
v1.11.B004	None
v1.11.B003	1. The switch console freezes if changing any STP-related configuration (e.g., enable/disable STP ports, or reset configure). 2. The MST ID can not be configured correctly by WEB UI. 3. While one port leaves MLD snooping group, it will cause other ports to leave the group automatically. 4. Add the parameter "replace_DSCP " on ACL profile Ethernet, IP, Packet content mask and IPv6. 5. The switch can not add entry for IP-MAC-Binding via D-View module. 6. Single IP Management: The Commander switch with D-Link WEB GUI 1.0 can not manage SIM members with new D-Link WEB GUI 2.0. 7. The IP-MAC-Binding entry is created via SNMP even when MAC and port information are not provided. 8. When the "forward_unregeisted_group" is enabled, if one PC joins the group, the other PC connected with DGS-3200 can still receive the non-join mutlicast group data. 9. The client can not join MLD v2 group by using 'filter exclude null IP source' and can not leave group by using filter include null IP source. 10. A MLD v2 client can not leave a group if other group member keeps sending join packet. 11. The NDP packets can not pass through DGS-3200-10 while "filter_unregistered_group" is enabled. 12. Switch only sends one Robustness control packet when the switch receives leave packet, no matter what Robustness value has been set, either the switch is in querier or non-querier state. 13. The entry of MLD snooping table is not deleted even the client sends leave packet. 14. When receiving group specific query, the switch duplicates one extra query packet to its VLAN member ports. 15. The switch does not delete the entry of the IGMP snooping table, even it has received IGMP leave packets from clients.

v1.11.B003	16. Inconsistent GVRP information between Web-GUI and CLI. When the client disables VLAN advertisement under CLI or Telnet, it will show 'enable' on Web-GUI. 17. The switch can not flood router advertisement, neighbor advertisement or IPv6 PIM to all ports of the VLAN, when the switch learned router port in IPv6 environment. 18. If the client sends IGMP snooping/MLD snooping join packet first then the switch learns a router port, the switch will not flood the multicast traffic to router port. 19. While SSH server is enabled on DGS-3200-10, telnet client can not work. 20. The switch can not add 2nd and 3rd RADIUS servers. 21. When using MAC-based Access Control to authenticate a client, the switch does not assign correct VLAN to the client even when it is successfully authenticated. 22. Fix head of line blocking problem. If there are too many broadcast, multicast or unknown traffics, the packet will be lost. 23. Change "cold-start" to "warm-start" in SNMP.
v1.00.B015	First release

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues
V2.00.016	None
V1.50.B052	1. The incorrect report will be learned to IGMP table. 2. IGMP leave message will affect different groups. 3. Cannot configure limited multicast address range with the same name of the created profile. 4. Data driven learning table cannot update after deleting the multicast filter profile. 5. Limited multicast address range cannot block multicast group correctly. 6. DGS-3200-16 fiber port LED will be still displayed if the fiber of combo port disabled by software.
V1.50.B019 V1.35.B023	Per-port bandwidth control and per-flow bandwidth control are mutually exclusive on the same port.
V1.11.B004	None
V1.11.B003	None
V1.00.B015	First Release

Related Documentation:

- DGS-3200 Series User Manual
- DGS-3200 Series CLI Manual
- DGS-3200 HW Installation Guide