Firmware Version: V3.00.B14
Prom Code Version: V1.10.B09
Published: 2012/12/10

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.

For more detailed information regarding our switch products, please refer to Related Switch 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: v3.00.B14 Prom: v1.10.B09	2012/12/10	DGS-3612	A1, A2
		DGS-3612G	A1, A2
		DGS-3627	A1, A2
		DGS-3627G	A1, A2
		DGS-3650	A1, A2, A3
Runtime: v2.80.B31 Prom: v1.10.B09	2010/7/1	DGS-3612	A1
		DGS-3612G	A1
		DGS-3627	A1
		DGS-3627G	A1
		DGS-3650	A1, A2
Runtime: v2.50.B51 Prom: v1.10.B09	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:

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.

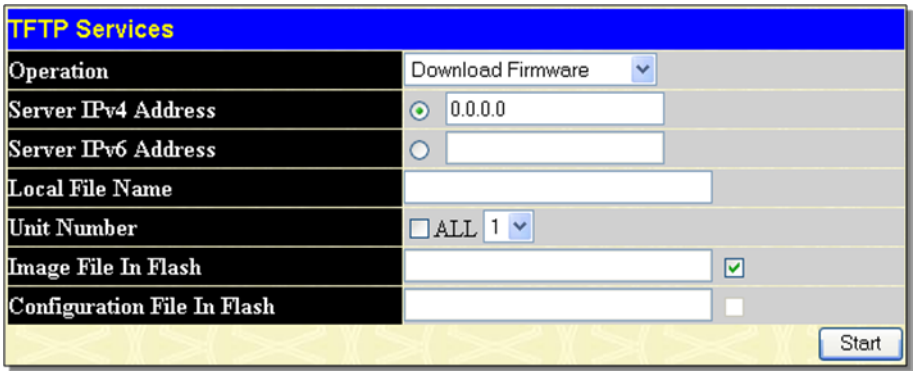
Example:

```
DGS-3627:5# download firmware_fromTFTP 10.53.13.201 R280B31.had c:\ firm1
Command: download firmware_fromTFTP 10.53.13.201 R280B31.had c:\ firm1

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

DGS-3627:5# config firmware c:\ firm1 boot_up
Command: config firmware c:\ firm1 boot_up

Success.

The switch:5# show boot_file
Command: show boot_file
--------------------------------------------------
 Unit ID : 1
 Boot up firmware image : C:\firm1
 Boot up configuration file: C:\STARTUP.CFG
 --------------------------------------------------

The 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...
```

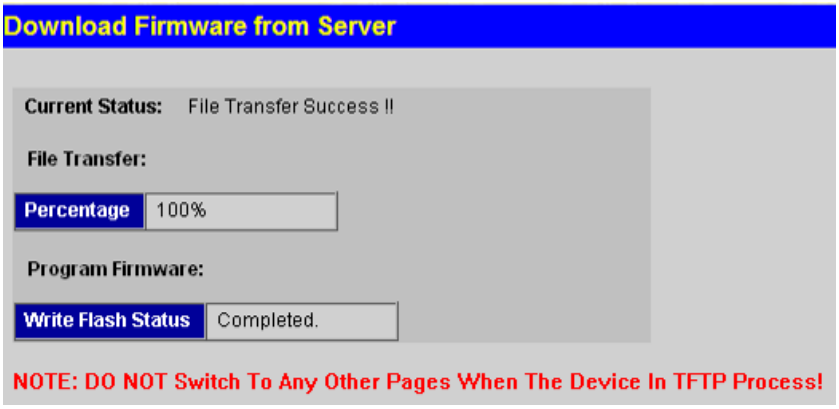
Upgrading by using Web-UI

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.

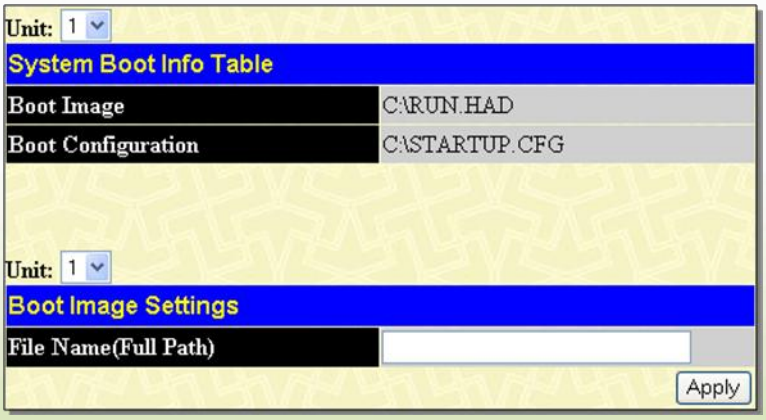
To update the switch's firmware or configuration file, click **Administration > TFTP Services** in function tree.



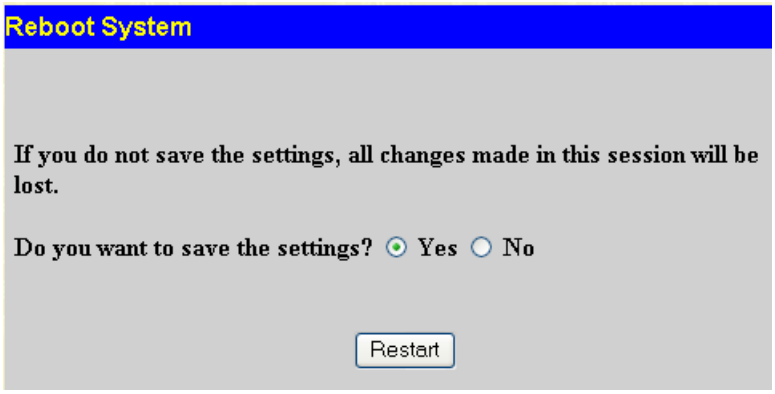
4. Select Download Firmware in **Operation.**
5. Select the type (IPv4 or v6) of IP address of the TFTP server and enter the IP address.
6. Fill in **Local File Name** with the name of the firmware file located on the TFTP server.
7. If the switch is under stacking mode, select the unit ID that you would like to upgrade the firmware.
8. Enter 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 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.
13. To reboot the switch, select **`Reboot System`** in the function tree.
14. Select "**Yes**" and click "**Restart**" button to reboot the switch.



New Features:

Firmware Version	New Features
V3.00.B14	1. LLDP-MED 2. Switch IP interface support /31 prefix 3. PIMv6 4. MLD 5. Support OSPF "distribute_list_in" parameters 6. OSPF support point-to-point type 7. DHCP client support option 12 8. PIM support loopback interface 9. Support VLAN_ID mask in ingress ACL and CPU ACL 10. Enhance the information of "show ospf lsdb" command 11. IPv6 static route redistrbute to OSPFv3 12. Support to disable a trunk member port 13. ERPS enlarge to 12 rings (instances) 14. LBD v4.05 15. Support IPv6 route longer than 64bit prefix 16. Policy route support "route_preference [default | pbr]" command 17. PIM support passive mode 18. Enhance password encryption support "community_encryption" command 19. DHCPv6 prefix delegation 20. One OSPF "link state update" packet carry multiple "link state advertisement" entries 21. Enhance the information of "show ports <portlist> media_type" command 22. Support null route redistribute to dynamic routing protocol 23. Super VLAN enlarge to 4, Sub-VLAN enlarge to 128 per Super VLAN 24. Support show DDM TX/RX power 25. Support display CPU port statistics 26. Support storm control log/trap for drop mode 27. Support enable/disable password recover 28. Support enable/disable MAC based access control per VLAN 29. Support jumbo frame per port 30. Support "boot time" display 31. Support "Ctrl" + "C" to interrupt traceroute 32. Secondary IP interface support Super VLAN 33. Enlarge to 1K IGMP static group 34. Y.1731

	35. IEEE 802.1ag CFM 36. PIM-SSM 37. DHCP server support option 43 38. Support configurable DHCP server option 39. SNTPv6 40. DSCP to CoS mapping 41. DHCP server support 8 pools 42. Support user privilege by TACACS+ authorization 43. DHCP server support static 256 binding records **NOTE:** All above features only support CLI
v2.80.B31	1. Configuration enhancement: ● Support the filtering keywords: include/exclude/begin when using "show config" and "upload_config" ● Support "increment" option when downloading cfg_fromTFTP If "increment" is specified, then the existing configuration will not be cleared. The new configuration will cover the existing configuration. ● Allow to specify "src_file"/"dst_file"/ "domain_name" in download/upload functions 2. Show memory/flash utilization 3. Show technical_support This command is especially used by the technical support personnel to dump the device overall operation information. The information includes the following information. Basic System information system log Running configuration Layer 1 information Layer 2 information Layer 3 information Application OS status Controller's status 4. Stacking enhancement: ● "Change Stacking priority" can work without reboot ● Stacking force master role feature This command 'config stacking force_master_role state enable' is used to ensure the master role is unchanged ● Hot insert/Hot Remove trap/log messages include MAC information ● Add new log/trap about topology change and role change ● Show stack information and show log include information about stacking topology 5. Send a trap while firmware upgrade via SNMP is finished. 6. Display user-understandable account level in CLI prompt DES-XXXX:3# -> DES-xxxx:user# DES-XXXX:4# -> DES-xxxx:oper# DES-XXXX:5# -> DES-xxxx:admin#. 7. CLI Command logging 8. Password recovery: allows to recover the password if the password is forgotten 9. Password encryption: allows to encrypt the password in configuration file 9. 8-level system log

10. Enlarge the number of trusted hosts to 30
11. SNMP-server & syslog source-interface appointment : allows to select an IP interface as the source interface to send syslog or trap message.
12. MEF certification
13. STP enhancement:
    - 802.1D 2004 RSTP
    - 802.1Q 2005 MSTP
    - STP Root Restriction
    - Source MAC of BPDUs uses port MAC instead of system MAC
    - Support edge port
    - Support BPDU address setting on NNI port when QinQ is enbled
    - Logging enhancement: The logs for stp topology changes include port and MAC-address
    - Log / show / debug Enhancement
14. D-LINK Unidirectional Link Detection (DULD)
15. Source MAC of L2 protocols (ERPS/LACP/STP/LBD) uses port MAC instead of system MAC
16. LACP support load-balancing with multicast traffic
17. Cable Diagnostics
18. Support "details" and "media_type" parameters in "show ports" command
19. Storm control enhancement:
    - Change "countdown" to "3-30"
    - Change "time_interval" to "5 - 600"
    - Auto recovery for the shutted-down port
20. Add 4 counters to gather statistics of various frame sizes, such as 1519-1522, 1519-2047, 2048-4095, 4096-9216
21. Mirror enhancement:
    - Multiple sessions of mirroring
    - Link aggregation ports can be set as a target port
22. sFlow enhancement:
    - Allow to specify ipv6 server
    - Support TX flow sampling
23. Microsoft NLB support.
24. IGMP/MLD snooping enhancement:
    - Support IGMP snooping Report suppression
    - Support static IGMP snooping group
    - Support MLD Snooping Host-based Fast Done
    - Support IGMP Snooping Host-based Fast Leave
25. ISM-VALN enhancement:
    - Support Tagged / Untagged member ports
    - Support Tagged / Untagged source ports
    - Configurable Multicast VLAN priority
    - Do not limit the number of total multicast addresses per ISM-VLAN entry when using "config igmp_snooping multicast_VLAN_group"
26. Forward protocol packets even the switch is under "filter_unregister_group mode" (Protocol packet: the packets with destination IP address in the range of reserved multicast addresses: 224.0.0.x, such as OSPF hello, PIM hello, and DVMRP probe etc.)
27. Support new OID to clear dynamic FDB by port/by VLAN

28. VLAN Trunking
29. Subnet-based VLAN
30. BPDU Attack Protection
31. ERPS (ITU-T G.8032 Ethernet Ring Protection Switching): support 2 rings
32. Super VLAN
33. ACL supports "IPv6 IP + UDP/TCP port" together.
34. Per queue egress bandwidth control.
35. WAC enhancement:
    - Identity driven policy assignment: Can assign ingress/egress bandwidth control, ACL and 802.1p default priority to the port according to the attributes dispatched from RADIUS server
    - Add log

      1) To record system stop learning and recovery from stop learning status when reaching the maximum entries

      2) To record authentication failure state for IPv4/IPv6
    - Support host-based authentication mode : assign ingress/egress bandwidth control for all hosts to the port; assign VLAN or 802.1p default priority to the host after successful authentication in host-based mode(R2.50 only supports assign VLAN in port-based)
    - Support IPv6
    - Support Per VLAN authentication
    - Support virtual IP: used to accept authentication requests from unauthenticated hosts. Only the requests sent to this IP will get response correctly.
    - Support time control for authenticated client (e.g. aging time/idle time/block time)
    - Support Authentication Database failover: Allows to configure the switch to check local database or bypass authentication when configured RADIUS server fails
    - Obsolete authentiation VLAN
    - Support compound authentication
36. Japanese Web-based Access Control (JWAC)
37. Compound authentication
38. ARP Spoofing Prevention
39. RADIUS accounting
40. RADIUS server setting supports ipv6
41. IP-MAC-Port Binding (IMPB) DHCPv6 Snooping
42. IP-MAC-Port Binding (IMPB) IPv6 ND Snooping
43. IP-MAC-Port Binding (IMPB) 3.8 which can prevent the netcut attack
44. MAC-based Access Control (MAC) enhancement
    - Enlarger the number of local database from 128 to 1024
    - Support Authentication Database failover: Allows to configure the switch to check local database or bypass authentication when configured RADIUS server fails
    - Support compound authentication
    - Support configurable per port/system maximum users
    - Delete the log when passing authentication.
    - Add four logs to record whether the port/system reaches to the maximum or recovers port learing.

      - MBAC enters stop learning state.

- MBAC recovers from stop learning state.
- Port < [unitID:]portNum> enters MBAC stop learning state.
- Port < [unitID:]portNum> recovers from MBAC stop learning state.

45. IP Directed Broadcast
46. ARP enhancement:
    - Show arpentry by mac address
    - Add OIDs to clear ARP
47. Loopback interface
48. BGP
51. OSPFv2 enhancement:
    - Enlarge OSPF neighbor to 64
    - OSPF areas are increased from 4 to 16
    - OSPF announces via loopback interface
    - OSPF enhancement (log/show/debug)
54. VRRP enhancement (log/show/debug)
55. Route enhancement:
    - Allow to configure route preference
    - Show ip route "hardware" option: display only the routes written into the chip.
56. Traceroute support ipv6
57. IPv6 Tunnel enhancement:
    - Support RA for ISATAP Tunnel
    - 6to4 Tunnel
    - Manual Tunnel
    - SATAP Tunnel
58. Display box and port information in "show ipv6 neighbor_cache"
59. RIPng
60. OSPFv3
61. DHCPv6 Server
62. DHCPv6 Relay
63. DHCPv6 Client
64. Ping enhancement:
    - Specify source IP address for ping request packet
    - Enalbe / disable broadcast ping reply
65. DNS Client
66. FQDN support - ping/tracert /tftp/telnet applications support fully qualify domain name.
67. Remote Copy Protocol (RCP) : allow users to copy firmware images configurations and log files between the Switch and RCP Server
68. SSH provides flexibility to change the default port number (22)
69. DHCP server: enlarge the DHCP pool entries to 1024 along with 8 pools
70. BOOTP/DHCP Relay:
    - Support DHCP local relay function that can insert option 82 information into DHCP broadcast packets from clients
    - Block recievied broadcast DHCP discover packets from flooding in local VLAN
    - DHCP Relay option 60 & 61
71. Traffic control auto recovery
72. Add traffic control "countdown" parameter: Timer for shutdown mode (only supported in CLI)
73. Change sFlow version from V1 to V5
74. Enable/disable cpu_rx_rate_control (only supported in CLI/MIB)

	75. Add digital signature in D-view module 76. Remove "Translate" option from OSPFv3 Area Settings
v2.50.B51	1. Port Security: maximum_learning_addr changes from 16 to 64. 2. IGMP source check : check the subscriber source IP when an IGMP report or leave message is received 3. Link aggregation ports can be set as a RSPAN target port in CLI 4. Plug/unplug the link aggregation member port, SNMP host can not receive SNMP trap.
v2.50.B25	1. Multicast static route 2. MAC-based access control 3. MAC-based VLAN 4. Loopback Detection (LBD) 4.0 5. Telnet client support 6. DHCP server screening 7. Proxy ARP 8. Support MTU configuration on IP interface 9. RSPAN 10. Per port configurable MDI/MDIX auto negotiation 11. L2 Protocol Tunneling (L2PT) 12. Selective QinQ 13. Serial number display support (Applicable from shipment loaded with this firmware) 14. Change floating static route behavior so that the primary route always has higher priority 15. OSPF ECMP route flag (Enable/Disable capability) 16. Add replace DSCP tag option on Ethernet type of ACL function 17. Change STP port forward BPDU default state to disabled 18. NAP-DHCP environment support 19. 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 Statistics
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. For detailed changes of MIB content, please refer to the modification history in each MIB file.

Firmware Version	MIB File	New Features
V3.00.B14	ZoneDefense.mib	Support ZoneDefense
	ie8021ag.mib	Support IEEE 802.1ag
	CFMEXTENSION.MIB	Support Y.1731
	LBD.mib	Support LBD v4.05
	L3MGMT.MIB	1. Support DHCP option 12 2. Support DHCPv6 client prefix delegation 3. IPv6 static route redistrbute to OSPFv3
	Genmgmt.mib	1. Support the configuration save/upload/download trap 2. Support total number of ARP entries 3. Port utilization by percentage
	time.mib	Add SNTPv6
	DHCPv6Server.mib	Support DHCPv6 server prefix delegation
	qinq.mib	Support configurable inner priority
	rfc4363.mib	Update RFC4363
	PIM-SM.mib	1. Support passive mode 2. Support PIM-SSM
	rfc4293.mib	Update RFC4293
	dhcpsever.mib	Support configurable DHCP server option
	ssh.mib	Support public key management
	ssl.mib	Support SSL intermediate CA certificate
	l2mgmt.mib	Add more information for SFP
	policyRoute.mib	Add "route_preference [default | pbr]" command
v2.80.B31	AAC.mib	1. Add SSH login and enable method
	ACL.mib	1. ACL supports "IPv6 IP + UDP/TCP port" together 2. Enlarge number of ACL profiles/rules
	AGENT-GENERAL-MIB	1. Enlarge the number of trusted hosts to 30
	ARPSpoofingPrevention.mib	2. ARP Spoofing Prevention
	Auth.mib	1. Support Per VLAN authentication 2. Support Authentication Database failover: Allows to configure the switch to check local

	database or bypass authentication when configured RADIUS server fails 3. Support compound authentication 4. RADIUS server setting supports ipv6 5. 802.1X ● Support "force log off (supported only in MIB)" ● Support "1X BPDU forwarding"" ● Support configurable maximum users feature per port/system (128/4000)
BPDUProtection.mib	1. BPDU Attack Protection
CableDiag.mib	1. Cable Diagnostics
DHCPServer.mib	1. DHCP server: enlarge the DHCP pool entries to 1024 along with 8 pools
DHCPv6Relay.mib	1. DHCPv6 Relay
DHCPv6Server.mib	1. DHCPv6 Server
DNSResolver.MIB	1. DNS Client
DULD.mib	1. D-LINK Unidirectional Link Detection (DULD)
Equipment.mib	1. "Change Stacking priority" can work without reboot 2. Stacking force master role feature 3. Show stack information and show log include information about stacking topology
ERPS.mib	1. ERPS: support 2 rings
Genmgmt.mib	1. Support "increment" when using "download cfg_fromTFTP" 2. Allow to specify "src_file" / "dst_file" / "domain_name" in download/upload functions 3. Show memory/flash utilization 4. CLI Command logging 5. Support new OID to clear dynamic FDB by port/by VLAN 6. Support new OIDs to clear ARP 7. Enable/disable broadcast ping reply 8. FQDN support - ping/tracert /tftp/telnet applications support fully qualify domain name. 9. Log/Trap eight level support 10. Support "details" and "media_type" parameter in "show ports" command
IGMPv3.mib	1. Support IGMP Subscriber Source Network check.
IPMacBind.mib	1. IP-MAC-Port Binding (IMPB) DHCPv6 Snooping 2. IP-MAC-Port Binding (IMPB) IPv6 ND Snooping 3. IP-MAC-Port Binding (IMPB) 3.8 which can prevent the netcut attack
IPv6StaticRoute.mib	1. Allows to create static route for IPv6 tunnel feature
JWAC.mib	1. Japanese Web-based Access Control (JWAC)
L2mgmtDGS3612.mib L2mgmtDGS3612G.mib L2mgmtDGS3627.mib L2mgmtDGS3627G.mib	1. Mirror enhancement: ● Multiple sessions of mirroring ● Link aggregation ports can be set as a target port

	L2mgmtDGS3650.mib	2. Support IGMP snooping report suppression 3. Support static IGMP snooping group 4. Support IGMP Snooping Host Based Fast Leave 5. Support Tagged / Untagged member ports 6. Support Tagged / Untagged source ports 7. Configurable multicast VLAN priority 8. Do not limit the total number of multicast addresses per ISM-VLAN entry when using "config igmp_snooping multicast_VLAN_group" 9. VLAN trunking 10. Per queue egress bandwidth control. 11. Port Security: changes maximum_learning_addr from 16 up to 64. 12. Support DHCP local relay function that can insert option 82 information into DHCP broadcast packets from clients 13. Enable/disable cpu_rx_rate_control (supported only in CLI/MIB) 14. Support "details" and "media_type" parameters in "show ports" command
	l3mgmtDGS3612.mib l3mgmtDGS3612G.mib l3mgmtDGS3627.mib l3mgmtDGS3627G.mib l3mgmtDGS3650.mib	1. IP Directed Broadcast 2. Loopback interface 3. OSPF areas increase from 4 to 16 4. OSPF announces via loopback interface 5. Allow to configure route preference 6. DHCPv6 Client 7. DHCP Relay option 60 & 61
	mba.mib	1. MAC-based Access Control: ● Enlarge the number of local authentication entries from 128 to 1024 ● Support dynamic 802.1p, rate-limiting, assignment after successful authentication (with both Port-based and Host-based); R2.35 only supports VLAN assignment; ● Support configurable system/port maximum user (4000/4000) ● ● Enlarge MBAC Local DB to 1024
	MldSnp.mib	1. Support MLD Snooping Host-based Fast Done
	Nlb.mib	1. Microsoft NLB support
	MSTP.mib	1. Support 802.1D 2004 edition 2. Support STP 1Q 2005 MSTP 3. STP Root Restriction 4. Support the BPDU address setting on NNI port when QinQ is enabled
	PktStormCtrl.mib	1. Storm control enhancement: ● Change "countdown" to "3-30" ● Change "time_interval" to "5 - 600" ● Auto recovery for shutted-down port
	QinQ.mib	1. QinQ enhancement: be able to map inner priority to outer priority
	RADIUSAccounting.mib	1. RADIUS accounting
	RCP.mib	1. Remote Copy Protocol (RCP) : allow users to

		copy firmware images, configurations and log files between the Switch and RCP Server
	RFC1213.mib	1. Show arpentry by MAC address 2. Microsoft NLB support
	RFC2925P.mib	1. Allow to specify source IP address for ping request packet 2. FQDN support - ping/tracert /tftp/telnet applications support fully qualify domain name. 3. Specify source IP address for ping request packet 4. Add IPv6 ping
	RFC2925T.mib	1. FQDN support - ping/tracert /tftp/telnet applications support fully qualify domain name. 2. Add IPv6 traceroute
	RFC4087.mib	1. IP Tunnel enhancement
	RFC4273.mib	1. BGP
	RFC4363Q.mib	1. Add a MIB to create static FDB
	RFC5643.mib	2. OSPFv3
	RIPng.mib	1. RIPng
	sFlow.mib	1. sFlow enhancement: ● Support ipv6 server ● Support TX flow sampling 2. Change sFlow version from V1 to V5
	SSH.mib	1. SSH provides flexibility to change the default port number (22)
	SrcIPIf.mib	1. SNMP-server & syslog source-interface appointment: allows to select an IP interface as the source interface to send syslog or trap message.
	SuperVLAN.mib	1. Super VLAN
	SubnetVLAN.mib	1. Subnet-based VLAN
	WAC.mib	1. WAC enhancement: ● Identity driven policy assignment: Can assign ingress/egress bandwidth control and 802.1p default priority to the port according to the attributes dispatched from RADIUS server. ● Support host-based authentication mode : assign ingress/egress bandwidth control for all hosts to the port; assign VLAN or 802.1p default priority to the host after successful authentication in host-based mode(R2.50 only supports assign VLAN in port-based) ● Support IPv6 ● Support virtual IP: used to accept authentication requests from unauthenticated hosts. Only the requests sent to this IP will get response correctly. ● Support time control for authenticated client (e.g. aging time/idle time/block time) ● Can enable/disable WAC authentication state
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	

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
V3.00.B14	None
v2.80.B31	1. Delete the old WAC command: config wac VLAN If the user have configured WAC VLAN in the old firmware, when upgrading to the new firmware, he does not need to configure it again because WAC Authenticated ports will be reserved 2. download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {dest_file {{unit [<unitid 1-12> | all]} <drive_id>} <pathname 64> {boot_up}} | cfg_fromTFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {[dest_file {<drive_id>} <pathname 64> |increment]}] 3. upload firmware_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {src_file {<drive_id>} <pathname 64>}} Note: From v2.8 onward, 2 parameters (src_file, dest_file) are added. This improvement is to avoid potential command parsing problem. If you have upgraded the firmware to V2.80 or onward, and are using script to manipulate firmware or config file, please do not forget to add those 2 parameters to the script.

Problem Fixed:

Fixed Revision	Problems
V3.00.B14	1. DGS-3600 will delay the IGMP join packet when it is received too many SSDP packets (destination= 239.255.255.250). (DRU20111117000011)

	2. The port 27 (10G port) is displayed as "Disabled", but packets can pass through this port. (DRU20120217000003) 3. The priority of loopback interface is lower, sometimes "ping loopback interface" was no response.(DEUR20111207000007) 4. DGS-3627G entered the exception mode when LLDP code error was happened. (DRU20120601000003) 5. DGS-3627 BGP community command was not written into configuration correctly. (DRU20120618000008) 6. When doing "save" command via telnet, the telnet session maybe hang up. (DRU20120529000002) 7. The client can't join multicast group when Q-in-Q and IGMP Snooping are enabled simultaneously. (DRU20120712000002)
v2.80.B31	1. When telneting to the switch and enter the command 'sh tech_support', the switch may enter EXCEPTION MODE. (DI20091224000005) 2. sFlow may not represent the correct value of Output_interface_index. (DI20100114000010) 3. After running for 2~3 weeks, the switch's management interface can not be accessed. But all VLANs, QinQ and GVRP work well. (DRU20100309000002) 4. DGS-3627G can not learn default route via OSPF when disconnecting 10G cable from another OSPF Router. (DI20090806000010) 5. In a stable STP topology, if the Root Bridge's priority is changed to lower one, the STP Topology is unstable for a while and a loop condition appears. (DI20090908000007) 6. System IPIF does not respond to packets from PC connected on Stacking Member after 'reset config' 7. The bandwidth control does not work correctly with the values100M bit/s, 150M bit/s, 200M bit/s. (DEUR20091201000002) 8. When there are mixed IGMPv2 and IGMPv3 reports, the device will not send query packet when an IGMPv3 client sends leave packet. (DI20091216000019) 9. When pinging to switch in the speed of 1000 pkts/sec, with TTL =1, There are 723 packets lost. (DI20091223000005) 10. The device sends out the RADIUS packets with incorrect NAS-Identifier. It should be "D-Link". (DI20091217000006) 11. The device sends many same SNMP traps and syslog packets regarding to RSTP Topology change when Topology Change occurred on the LAG port across stacking units. (DI20100125000020) 12. The device can not be accessed when the loopdetect function VLAN base mode detects loop happening. (DT20100128000001) 13. The device freezes and is unavailable to be accessed via any of its interfaces except its console interface when DGS-3600 is used as L3 switch connected to access switches DES-3026, DES-3028 or ES-2024A. (DI20100215000007) 14. The device will automatically relay the DHCP discover packets via system IP interface when the VLAN that the client resides does not have IP interface and on which dhcp_relay is not enabled. (DRU20100316000006) 15. The device does not erase IGMP Snooping entries on LACP port. (DI20091110000013) 16. The device will not be able to send warmstart SNMP trap if the SNMP host resides in the different subnet than DGS-3600 does. (DI20100108000013) 17. After entering "ping6" command and pressing down "Ctrl+C" or "Esc" to exit quickly, the ping6 session will fail to close. If the user does this for more than 5 times, it will display "Ping6 task is busy !". (HQ20100106000005) 18. DHCP server would receive duplicate discover or request packets when the

	DHCP packet traverses via 2 cascading switches both with DHCP Relay enabled. (DI20091130000004) 19. The device responds with incorrect value to SNMP enquiries and sends abnormal trap when attaching the redundant power supply (DEUR20091016000006) 20. When using SNMP commands to create/delete policy route, the CPU utilization will be up to 80%. And after 5 hours working (or more), there will be no response and only rebooting it can solve the problem. (DI20091005000007) 21. It takes around 10 minutes to apply change for MSTP instance priority after setting new priority to the stack slave unit. (DI20091130000004) 22. DGS-3600 can not use ipv6 for web access management, but can be telneted by IPv6 address.(DT20090520000001) 23. When customer tries to create ACL rule with access_id auto_assign via SNMP, the rule can not be created.(DI20090708000024) 24. The device's throughput is low with 4 test PCs each with 1G connection (DT20090906000001) 25. A client PC with MAC and IP in device's IMPB white list can not ping to a device IP interface which is not bound with system MAC address. (DI20091013000005) 26. The client joins the multicast group and the traffic can be received by client properly. But after the port to the client links down/links up and the client will not able to receive the traffic anymore. (DI20091117000008) 27. When unplugging/plugging the uplink cable between the PIM-SM BSR switch and multicast source switch (RP), the client directly connected to the RP will stop receiving traffic for few seconds and then be back to normal. (DEUR20100324000002) 28. After 'enable clipaging' and 'show config active', the switch will flush about 68 lines at one page. It should be 25 lines per page by default. (DI20100324000001) 29. The SFP port in DGS-3612/3612G may sometimes go down and never recover. (DI20100104000003) 30. The stack will be corrupted after running around one day in the test environment with PIM/DM and IGMP_Snooping enabled. (DI20091216000009) 31. The device will reboot if checking the LLDP information via WEB interface and this issue only happens when connecting with Cisco ME2400. (DI20090915000023) 32. The receiving multicast RIP packet was trapped to CPU and did not be forwarded to another RIP enabled switch or server in the same network. (DRU20100413000001) 33. L2 multicast traffic can not transit through another link to PIM DR when the default link downs. (DI20080625000017) 34. ISM VLAN can not recognize IGMPv3 join packets
v2.50.B51	1. **The switch can not be upgraded with a firmware file larger than 4MB.** 2. It takes a long time to logout IX2000(router) when telneting IX2000 from DGS-3650. (DI20091013000002) 3. When using RIP to learn dynamic routing entries, the subnet mask becomes 32. The correct one should be 24. (DI20090910000012) 4. The user can not configure the VLAN forbidden ports in the ports which is configured as untagged member ports via SNMP.(DI20100129000019) 5. When the master unit's power is cut off, the stacking member switches do not respond to SNMP Get Request correctly. For example, if the Unit1's power is cut off and Unit2 becomes the master unit, the Unit1's port

	information still can be seen. (DI20091217000006) 6. The DHCP clients sometimes fail to get the IP address from DHCP server when using DHCP Relay function.(DI20090519000007)
v2.50.B25	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 can not refresh by pressing F5. 4. Firefox 3 can not 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 can not 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 can not 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 can not 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 can not 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 can not access network. 24. Power_ notification_trap does not respond correctly 25. When using SNMPwalk to get the FDB information from the switch, DGS-3600 can not respond correct information if there are over 1K MAC under this interface.
v2.40.B19	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.If the size of the config file is more than 2M, the device will lose some config.
v2.20.B38	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 can not classified the IP address correctly when the address including the number "255", for example, 172.30.255.254/16 7. DGS-3600 can not 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 can not 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 can not 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 makes 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
V3.00.B14	1. After changing path of PIM-SSM, some multicast streams are not forwarded if there are more than 128 groups joined. 2. Some failover operates (such as disable/enable PIM6, disable/enable interface, hot remove/insert unit, power off/on some units) maybe cause PIM6 forward packet abnormal, only reboot can be solved.	None
v2.80.B31	1. When powering off/on a stacking member unit, the STP topology was changed and the stacking unit is sometimes in loop condition for a while. (DI20100514000005) 2. OSPFv3 state is not synchronous after removing then inserting the slave unit. IPv6 packets may be forwarded incorrectly 3. The device may crash when linking down OSPFv3 normal and virtual neighbours one by one 4. BGP may crash when linking down then up the stacking cable after one day's running and also may crash when clearing dampening with 10000 routes	None
v2.50.B25	1. MTU setup does not support multicast. 2. In stacking mode with PIM-SM and IGMP enabled, CPU utilization may be up to 100% when more than 512 groups are being forwarded. 3. If RSPAN mode is TX, the monitored packets will take double tags with RSPAN source vlan when the packets egress form tagged destination port. 4. Some protocol packets such as OSPF hello packets can still be mirrored to the destination port when there is no redirected port in the destination switch.	None
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 than 1500 bytes 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. Upgrade to R2.80.B31 or above. 2. None 3. None 4. None 5. None
V2.20.B38		
v1.00.B66	1. If the size of the config file is more than 2M, the device will lose some config. 2. Chip Limitations: ●Flow control can support "5 ports to 1 port" at best. ●For egress mirroring, the target port will always	1. Upgrade to R2.40.B19 or above. 2. None

	receive "tagged" packets. ● "CPU interface filtering" can not filter source MAC address.	

Related Documentation:

DGS-3600 Series User Manual
DGS-3600 Series CLI Manual