Firmware Version: V3.00.B14
Prom Code Version: V1.00.B13
Published: Nov.26,2012

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:

Firmware Version	Date	Model	Hardware Version
Runtime: V3.00.B14 Prom: v1.00.B13	26-Nov-12	DGS-3426	A1, A2, A3
		DGS-3426P	A1, A2
		DGS-3427	A1, A2, A3
		DGS-3450	A1, A2, A3
Runtime: V2.70.B56 Prom: v1.00.B13	30-Jun-10	DGS-3426	A1, A2, A3
		DGS-3426P	A1, A2
		DGS-3427	A1, A2, A3
		DGS-3450	A1, A2, A3
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 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 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> {image_id <int 1-2>}]	Download firmware file from the TFTP server to the switch.
config firmware image_id <1-2> [delete | boot_up]	Change the boot up image file.
show firmware_information	Display the information of current boot image and configuration.
reboot	Reboot the switch.

Example:

1. DGS-3426P:5#download firmware from TFTP 10.90.90.91 R270B56.had image_id 2

```
Command: download firmware_fromTFTP 10.90.90.91 R270B56.had image_id 2

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

2. DGS-3426P:5#config firmware image_id 2 boot_up

```
Command: config firmware image_id 2 boot_up

Success.
```

3. DGS-3426P:5#show firmware information

```
Command: show firmware information

ID  Version    Size(B) Update Time          From              User
 -- --------- ------- ------------------- ----------------- ---------------
  1  2.60.B26  2450452 2010/02/04 17:00:26  10.90.90.91(R)     Anonymous
 *2  2.70.B56  4029512 2010/03/05 02:25:85  10.90.90.91(R)     Anonymous

'*' means boot up firmware
(R) means firmware update through Serial Port(RS232)
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SSH) means firmware update through SSH
(SIM) means firmware update through Single IP Management
```

4. DGS-3426P:5#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.B13
--------------------------------------------------------------------------------
```

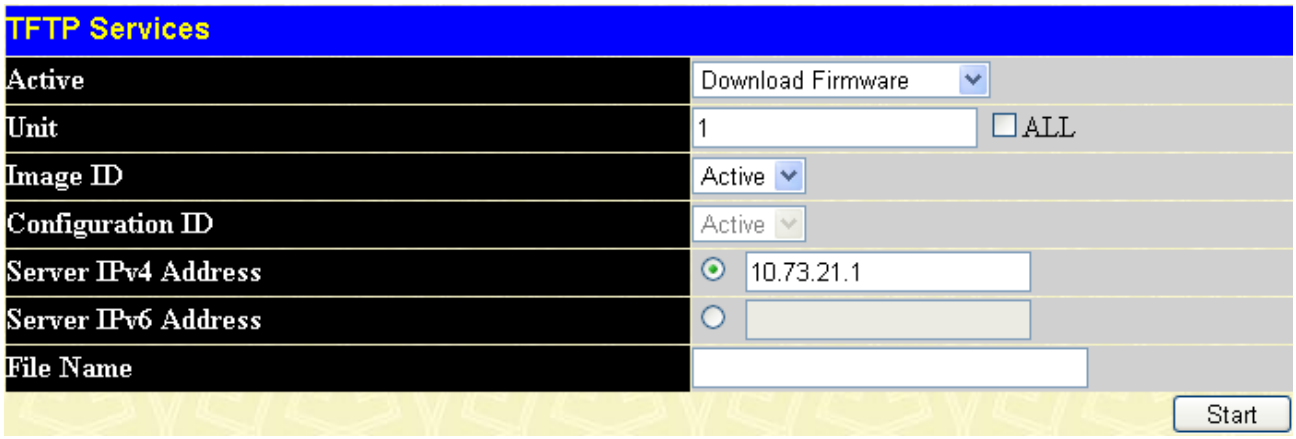
```
Power On Self Test ....................................  100 %

MAC Address   : 00-1E-58-4F-F7-D0
H/W Version   : A1

Please wait, loading V2.70.B56 Runtime image .............   100 %
UART init .........................
Device Discovery .....................................  100 %
Configuration init ...................................  100 %
```

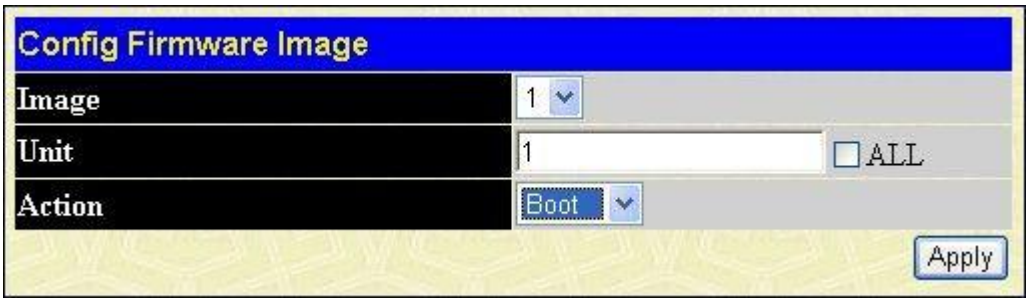
Upgrade using Web-UI

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 the switch's firmware or configuration file, select **Administration > TFTP Services** in function tree. Select Download Firmware in **Operation**.

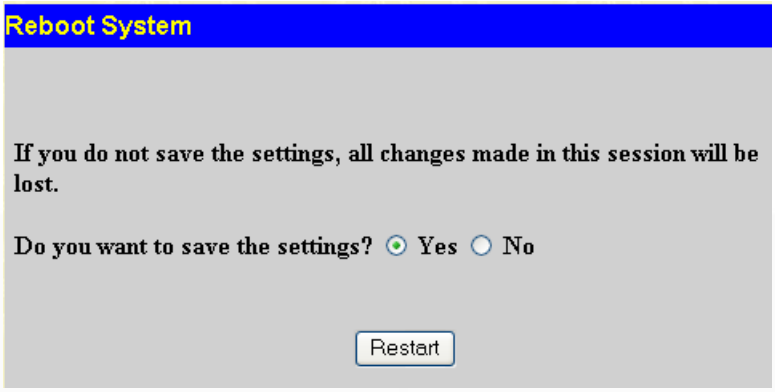


5. If the switch is under stacking mode, select the Unit ID of the switch that will be upgraded.
6. Select the **Image ID** of the firmware. Choosing *Active* will download the firmware to the Boot Up Image ID.
7. Select the type (IPv4 or IPv6) of IP address of the TFTP server and enter the IP address.
8. Enter the firmware file name in **File Name**.
9. Click "**Start**"
10. Wait until the "File Transfer" status reaches **100%** and the "Program Fi**rmware"** status shows "**completed**".

11. To select the boot up image used for next reboot, click **Administration > Multiple Image Services > Config Firmware Image** in the function tree.



12. Enter the image ID and choose "Boot" then click "**Apply**".
13. To reboot the switch, click DGS-3400 Web Management Tool > Reboot System. Select "***Yes"*** and click "***Restart***" button to reboot the switch.



New Features:

Firmware Version	New Features
V3.00.B14	1. Y.1731 2. IEEE 802.1ag CFM 3. Private VLAN 4. D-Link Voice VLAN v2.0 5. DHCP client support option 12 6. DHCP server support option 43 7. ERPS enlarge to 12 rings (instances) 8. SNTPv6 9. LLDP-MED 10. Time-based PoE 11. DHCPv6 Prefix Delegation 12. Support packet counter for stacking port 13. Support to disable a trunk member port 14. Enhance the information of "show ports <portlist> media_type" command 15. Support SSL intermediate CA certificate 16. Support storm control auto-recover mode. 17. Support jumbo frame per port 18. Support "Ctrl" + "C" to interrupt traceroute 19. Support "boot time" display 20. Support public key for SSH authentication 21. Support VLAN_ID mask in ingress ACL and CPU ACL 22. DSCP to CoS mapping 23. Support show DDM TX/RX power 24. Support enable/disable MAC based access control per VLAN 25. Support IPv6 route longer than 64bit prefix 26. Support JWAC/WAC authentication page for iOS/Android smartphone 27. LBD v4.05 28. Support configurable DHCP server option 29. Enhanced password encryption support "community_encrytion" 30. CLI command history logging 31. Support display CPU port statistics 32. Switch IP interface support /31 prefix **NOTE:** All above features only support CLI
V2.70.B56	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.
   This command can show CLI command setting history.
8. 8-level system log
9. Password recovery: allows to recover the password if the password is forgotten.
10. Enlarge the number of trusted host 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. 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
13. D-LINK Unidirectional Link Detection (DULD) function.
14. Source MAC of L2 protocols (ERPS/LACP/STP/LBD) uses port MAC instead of system MAC
15. LACP support load-balancing with multicast traffic.
16. Storm control enhancement:
    - Change "countdown" to "3-30".
    - Change "time_interval" to "5 - 600".
    - Auto recovery for the shutdown port.
17. Add 4 counters to gather statistics of various frame sizes, such as 1519-1522, 1519-2047, 2048-4095, and 4096-9216.

18. Mirror enhancement:
    - Multiple sessions of mirroring
    - Link aggregation ports can be set as a target port
19. sFlow enhancement:
    - Allow to specify IPv6 server.
    - Support TX flow sampling.
20. Microsoft NLB (Network Load Balancing) support.
21. Add "data driven group" in IGMP/MLD snooping.
22. ISM-VLAN enhancement:
    - Support Tag / Untagged member ports.
    - Support Tag / 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"
23. 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.)
24. Support new OID to clear dynamic FDB by port/by VLAN.
25. VLAN Trunking
26. Subnet-based VLAN.
27. BPDU Attack Protection.
28. ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) support.
29. ACL supports "IPv6 IP + UDP/TCP port" together.
30. Per queue egress bandwidth control.
31. 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
32. Japanese Web-based Access Control (JWAC) enhancement (support JWAC v2.02)
    - Show IP address and user ID in UI and log

- JWAC notification: Show notification to user automatically after passing the authentication.
- Administrator can use FQDN URL to access JWAC login page instead of using IP

33. Compound authentication
34. ARP Spoofing Prevention.
35. Radius server setting supports IPv6.
36. Increase "max_learning_addr" number in port security from 16 up to 64.
37. IP-MAC-Port Binding (IMPB) DHCPv6 Snooping
38. IP-MAC-Port Binding (IMPB) IPv6 ND Snooping
39. IP-MAC-Port Binding (IMPB) 3.8 which can prevent the netcut attack
40. 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.
41. IP Directed Broadcast.
42. ARP enhancement:
    - Show arpentry by mac address.
    - Add OIDs to clear ARP table
43. Proxy ARP.
44. RIPv1/v2.
45. Interface enhancement:
    - Support secondary IP in L3 interface.
    - Expand IP interface number from 32 to 64.
46. Route enhancement:
    - Allow to configure route preference
    - Show IP route "hardware" option : display only the routes written into the chip
47. Trace route supports IPv6.
48. IP Tunnel enhancement:
    - 6to4 Tunnel
    - Manual Tunnel
    - ISATAP Tunnel (Intra-Site Automatic Tunnel Addressing Protocol)
49. Display box and port information in "show ipv6 neighbor_cache".
50. RIPng.
51. IPv6 static route supports backup route.
52. DHCPv6 Server.
53. DHCPv6 Relay.
54. DHCPv6 Client.
55. Ping enhancement:
    - Specify source IP address for ping request packet
    - Enalbe / disable broadcast ping reply

	56. FQDN support - ping/tracert /tftp/telnet applications support fully qualify domain name 57. Remote Copy Protocol (RCP) : allow users to copy firmware images, configurations and log files between the Switch and RCP Server 58. DHCP server: enlarge the DHCP pool entries to 1024 along with 8 pools 59. DNS Relay. 60. DHCP/BOOTP 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 61. RSPAN (Remote Switched Port Analyzer) support: Can monitor and analyze the traffic passing through the ports in another switch. 62. IGMP Snooping supports 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. 63. Route redistribution: allows routers on the network, which are running different routing protocols to exchange routing information. 64. Enlarge MAC Base Access Control local DB to 1024. 65. Add traffic control "countdown" parameter: Timer for shutdown mode (only supported in CLI). 66. Update sFlow version from 1.00 (IPv4) to V5 (IPv6). 67. Add digital signature in D-View module. **Note:** Suggest user to reconfigure WAC again after upgrading firmware from R2.60 to R2.7
V2.60B26	1. Selective Q-in-Q -VLAN Translation 2. L2 Protocol Tunneling 3. LLDP 4. sFlow 5. IMPB v3.5 6. Web-based Access Control (WAC) -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 -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 -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

   -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

    -IGMPv3 Snooping

    -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

18. MLD Snooping enhancement

    -MLDv2 Snooping

    -MLD Snooping dynamic group entries changed from 1K to 511

19. L2 Multicast VLAN Replication (Static configuration): Admin can manually configure the switch to route multicast traffic across VLANs
20. STP Root Restriction (defined in 802.1Q-2005)
21. 802.1D-2004
22. Gratuitous ARP
23. Three-Level User Account
24. 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
25. 2nd IPv4 Static Default Route
26. DHCP Relay option 60 & 61
27. Password Encryption
28. DHCP-NAP support
29. Telnet Client
30. 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
31. Bandwidth Control enhancement
    -changes per-port min. granularity from 64kbps to 1kbps
32. Ping MIB
33. Traceroute MIB
34. Entity MIB
35. Can enable / disable SNMP State; default is disable
36. When primary route is active, always use primary route over backup route.
37. When DHCP Relay is enabled, the Switch will block all broadcast DHCP packets in the local IP Interface
38. LBD will send traps when loops are detected and recovered
39. Configurable SSH Server TCP port
40. When configuring static multicast_fdb, typing 01005exxxxxx or 333xxxxxxxx is not allowed
41. ipif_ipv6_link_local_auto can be enabled or disabled; default is disabled
42. Added parameter 'ip address' to the command "show iproute"
43. Admin can specify which Firmware image ID the switch will use during boot-up
44. Added an extra /y parameter for commands which prompt (Y/N)
45. 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.
46. 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) 47. Enabled "Show FDB" by VID as well as by VLAN Name 48. Enabled "Show VLAN" by VID as well as by VLAN Name 49. Web-based GUI: Changed D-Link logo's link to www.dlink.com.tw 50. Attack log will include IP address, MAC address and port number 51. Admin account can remove MAC address display from log 52. "Show Fan Status" command enhanced with log and trap 53. "Show STP ports" command is standardized for all slave and master switches in a stack 54. Added MIB for "Show Memory" usage and percentage (DRAM utilization, Flash utilization) 55. Added link up/down trap per port (RFC 2233) 56. Modified RPS MIB description and added traps 57. OID added to show port utilization 58. OID added to clear FDB and ARP table **Notes:** 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.
V2.35.B09	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	1. JWAC support 2. ISM VLAN 3. Inter-VLAN routing enhancement No need to manually configure host's MAC address
V2.00.B52	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
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
	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
	l2mgmt.mib	Add more information for SFP
	DHCPv6Server.mib	Support DHCPv6 server prefix delegation
	qinq.mib	Support configurable inner priority
	rfc4363.mib	Update RFC4363
	dhcpsever.mib	Support configurable DHCP server option
	ssh.mib	Support public key management
	ssl.mib	Support SSL intermediate CA certificate
V2.70.B56	ACL.mib	1. ACL supports "IPv6 IP + UDP/TCP port" together 1. Enlarge number of ACL profiles/rules
	AGENT-GENERAL-MIB	Enlarge the number of trusted hosts to 30
	ARPSpoofingPrevention.mib	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"" 6. Support configurable maximum users feature per port/system (128/4000)
	BPDUProtection.mib	BPDU Attack Protection
	DHCPServer.mib	DHCP server: enlarge the DHCP pool entries to 1024 along with 8 pools
	DHCPv6Relay.mib	DHCPv6 Relay
	DHCPv6Server.mib	DHCPv6 Server
	DNSResolver.mib	DNS Client

	DULD.mib	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	ERPS: support 2 rings
	Genmgmt.mib	1. Allow to specify "src_file" / "dst_file" / "domain_name" in download/upload functions 2. Show memory/flash utilization 3. CLI Command logging 4. Support new OID to clear dynamic FDB by port/by VLAN 5. Support new OIDs to clear ARP 6. Enable/disable broadcast ping reply 7. FQDN support - ping/tracert /tftp/telnet applications support fully qualify domain name 8. Log/Trap eight level support 9. Support "details " and "media_type" parameter in "show ports" command Support "increment" when using "download cfg_fromTFTP"
	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	Allow to create static route for IPv6 tunnel feature
	JWAC.mib	JWAC enhancement(support JWAC v2.02) ●Show IP address and user ID in UI and log ●JWAC notification: Show notification to user automatically after passing the authentication. ● System administrator can use FQDN URL to access JWAC login page instead of using IP
	L2mgmtDGS3426.mib L2mgmtDGS3426P.mib L2mgmtDGS3427.mib L2mgmtDGS3450.mib	1. Mirror enhancement: ● Multiple sessions of mirroring ● Link aggregation ports can be set as a target port 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
l3mgmtDGS3426.mib l3mgmtDGS3426P.mib l3mgmtDGS3427.mib l3mgmtDGS3450.mib	1. IP Directed Broadcast 2. DHCPv6 Client 3. DHCP Relay option 60 & 61 4. Add parameter in "show ports" command 5. Allow to configure route preference
mba.mib	MAC-based Access Control enhancement ● 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) ● Enlarge MBAC Local DB to 1024
Nlb.mib	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	Storm control enhancement: ● Change "countdown" to "3-30" ● Change "time_interval" to "5 - 600" Auto recovery for shutted-down port
RCP.mib	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	IP Tunnel enhancement ● 6to4 Tunnel ● Manual Tunnel ● ISATAP Tunnel (Intra-Site Automatic Tunnel Addressing Protocol)
RIPng.mib	RIPng
RSPAN.mib	RSPAN enhancement
sFlow.mib	1. sFlow enhancement: ● Support ipv6 server

		• Support TX flow sampling 2. Change sFlow version from V1 to V5
	SrcIPIf.mib	SNMP-server & syslog source-interface appointment
	SubnetVLAN.mib	Support subnet-based VLAN
	WAC.mib	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 Add log • 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
V2.60.B26	Q-in-Q MIB	Selective Q-in-Q
	Agent-MIB	Gratuitous ARP
	LLDP-MIB LLDP-dot-MIB LLDP-dot3-MIB	LLDP
	SFLOW-MIB	sFlow
	DHCP-Server-MIB	DHCP Server
	AUTH-MIB	1. Compound Authentication 2. 802.1X enhancement -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	1. Per-flow Bandwidth Control (ACL Flow Metering) -CIR (Committed Information Rate) -Two-rate Three Color Marker (TrTCM) -Single-rate Three Color Marker (SrTCM) 2. 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
	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 -MLDv2 Snooping
	IP-MAC-BIND-MIB	IMPB v3.5
	JWAC-MIB	JWAC enhancement -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) -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 -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	1. IGMP Snooping enhancement -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	1. DHCP Relay option 60 & 61 2. 2nd IPv4 Static Default Route 3. ipif_ipv6_link_local_auto can be enabled/disabled; disabled by default
	AGENT-GENERAL-MIB	1. Trusted Host enhancement -Can create trusted host not only for one IP but also for network range -Can delete all trusted host with one command 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	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
V3.00.B14	None
V2.70.B56	1. Modify the "show 8021x user" command to：”show 802.1x user” 2. Delete the old WAC command: config wac VLAN If you have configured WAC VLAN on firmware prior to v2.7, when upgrading to v2.7, you do not need to configure it again because WAC Authentication ports will be reserved 3. Change the command download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> {{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>]}] to 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]}] Note: From v2.7 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 V2.70 or onward, and are using script to manipulate firmware or config file, please do not forget to add those 2 parameters to the script.
V2.60.B26	None

Problems Fixed:

Firmware Version	Problems Fixed
V3.00.B14	1. After creating 4,000 VLAN and enabling MSTP, CPU utilization became to 100% for a while and it sometimes causes topology change or loop condition. (DI20100706000005) 2. When typing "reboot" command on a 12 device stack, DGS-3400 may enter exception mode. (DI20110104000007) 3. DGS-3400 will stop sending LACP and STP PDU packets around 3 seconds when dumping "tech_support" information. (DI20110308000001) 4. When getting ERPS value via SNMP, the packet will be padded with null-characters (DI20110405000002) 5. When deleting one VLAN, VLAN ID of "IGMP snooping static groups" is equal or larger than that VID will be deleted incorrectly too.(DRU20110715000002) 6. After enabling IGMP Snooping on DGS-3450, the PPPoE packets will be dropped by CPU. (DRU20111021000001) 7. When master unit is powered off in a stack, slave units will restart the ERPS and keep in blocking/idle state incorrectly (DI20111226000002, DI20120111000009) 8. When enabling IGMP Snooping, the IP-in-IP packet will be failed to pass through DGS-3400. (DRU20120530000002) 9. When enabling IGMP Snooping, ARP reply packet which is not to device was captured to CPU incorrectly. (DRU20120711000004)
V2.70.B56	1. Via SNMP, the counter value of the port will be 0 when the port is linked down (DI20090820000010, DI20090827000008) 2. When user logins via JWAC and continuously moves client PC on different ports, the switch session table will be full, and then the PC can not get IP address from the DHCP Server. User can see the log "JWAC enters stop learning state" (DI20090422000006). 3. After user links up/links down one port on DGS-3400, the SNMP host can not receive SNMP trap about link change from DGS-3400. (DI20090924000019) 4. Rebooting the slave stacking unit while JWAC authentication from clients are undertaken will cause the slave unit to show "Device Discovery" after its rebooting. (DI20091005000016) 5. DGS-3400 does not erase IGMP Snooping entries for LAG port (DI20091028000024) 6. DGS-3400 does not erase MLD Snooping entries for LAG port.(DI20091028000025) 7. Some stacking units are unstable when IMPB and DHCP snooping are enabled (DI20091109000006) 8. Some clients' IP addresses are not written to "binding_entry" table when 12 GDS-3400 are in a stack with IMPB and DHCP Snooping enabled. (DI20091111000007) 9. DGS-3400 does not flood IPv6 control packets when MLD Snooping is enabled. (DI20091028000013) (DI20091028000015) 10. When Topology Change has occurred on the LAG port over stacking units, DGS-3400 sends many SNMP traps and Syslog packets which are related to RSTP Topology change. (DI20100125000011) 11. JWAC Customized Page displays error after saving and rebooting the switch (DI20090921000002) 12. DGS-3426 may enter exception mode when configuring some SNMP commands (DI20100125000014) 13. Clients cannot be authenticated by JWAC, because DGS-3400 JWAC does not respond to the VLAN-tagged packets. (DI20090724000011) 14. If the SNMP manager sends "SNMP get request" about "ifNumber: 0" to

	DGS-3400, the value of response is incorrect. (DI20090813000010) 15. High CPU utilization issue (DUSA20090227000001) (1) When LACP runs across stacking units (total two stacking units), powering off the master unit will make LACP re-run and it needs around 5-7 seconds to recover. (2)After powering on the Master and reconnecting the Master back to the stack topology, the LACP will lose traffic around 1.7 second. (3)The DGS-3400 CPU utilization is up to 100% when receiving a lot of broadcast traffic. 16. Device will send out the RADIUS packets with NAS-Identifier not as "D-Link".(DEUR20100118000006) 17. The character in last line of uploaded configuration file is not 0x0D0A (DI20100309000013) 18. When using WindowsXP with window size 80*25 to telnet the device and then execute "show config", some command characters are missing if the command length is longer than 80. (DI20100316000008) 19. DGS-3400 series can not recognize Cisco STP packets thus STP port role and status are not changed when DGS-3400 is connected to a Cisco Switch (DI20100316000010) 20. Some MAC addresses are recorded as "BlockByMACAuth" even though these MACs are already authorized by MAC Base Access Control (MAC)feature as "Authenticated". (DI20091117000012). 21. When STP is enabled, DGS-3400 CPU utilization becomes 100% after unplugging and plugging the port connection between the stack master and slave. (DI20091119000008) 22. DGS-3400 CPU becomes high utilization when cleaning the IMPB entry (DI20100118000011) 23. 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)
V2.60.B26	1. When DGS-3400s are in stacking mode, powering off unit 1~5 and then powering them back will sometimes cause stack recovery failure. (DI20080818000001) 2. After user resets the switch and then enables stacking via Web GUI, the switch cannot be pinged. (DI20081224000007) 3. Web GUI does not display ACL rules correctly. (DI20090618000010) 4. Admin cannot use the CLI command "config double_vlan d169 add access 23" to add double VLAN access member port. (DT20081222000002) 5. SSH Login: When using OpenSSH 5.1p1 and a particular script file to test, the switch will enter exception mode. (DI20081106000011) 6. Loopback Detection (LBD) will not always activate if the loop traffic includes STP BPDU. (DI20081118000011)
V2.35B09	1. Sometimes Link Aggregation group does not function when stacking mode is enabled 2. Under certain setup the desired VLAN is not being assigned to authenticated wireless client but instead the AP's managed VLAN 3. In stacking mode, sometimes backup master will not become master when the master fails in a stack 4. Remove the PoE menu from Web GUI for non-PoE DGS-3400 models
V2.30B10	1. Single IP Management (SIM) only works with default VLAN 2. Password string display disclosed when the first character has been removed 3. Instability issue between Intel 10G NIC and DGS-3400 Series 10G modules (DEM-410CX) which causes link down/link up frequently

V2.00B52	1. User logins in through SSH successfully but log shows that both SSH login and console login event happen at the same time 2. Switch hangs when using Telnet to create 128 ACL rules 3. Wrong ACL OID is retrieved via snmpwalk tool 4. Syslog cannot accurately classify the severity of the message 5. Switch enters Exception Mode when saving through Telnet 6. Creating ACL via Web GUI will cause the web management to go down 7. Creating CPU filtering ACL will cause the web management to go down 8. SNMP compatibility issue at ACL with Firewall DFL-1600 9. Wrong warm_start trap type is sent while rebooting 10. 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	1. Modify the naming of "LoopBack Guard" to "Loopback Detection" on Web GUI 2. 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
V3.00.B14	DGS-3426P and SuperMicro AOC-SG-I2 Gigabit NIC has compatible issue. (DEUR20101029000004)	None
V2.70.B56	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)	None
V2.60.B26	**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	None

Related Documentation:

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