Firmware Version: V3.00.004
Prom Code Version: V1.00.016
Published: 2017/10/11

These release notes include important information about D-Link DGS-3620 series firmware revisions. Please verify that these release notes are correct for your switch:

- If you are installing a new switch, please check the hardware version on the device label; make sure that your switch meets the system requirement of this firmware version. Please refer to Revision History and System Requirement for detailed firmware and hardware matrix.
- If the switch is powered on, you can check the hardware version by typing "show switch" command or by checking the device information page on the web graphic user interface.
- If you plan to upgrade to the new firmware release, please refer to the Upgrade Instructions:
- D-Link switches support firmware upgrade via TFTP server. You can download the firmware from D-Link web site http://tsd.dlink.com.tw, and copy the downloaded firmware to the TFTP server folder. Please make sure that the TFTP server is accessible from the switch via networks. for the correct firmware upgrade procedure.

For more detailed information regarding DGS-3620 series 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: v1.00.035 Prom: v1.00.012	2011/3/25	DGS-3620-28TC	A1
		DGS-3620-28SC	A1
		DGS-3620-28PC	A1
		DGS-3620-52T	A1
		DGS-3620-52P	A1
Runtime: v1.00.038 Prom: v1.00.014	2011/5/13	DGS-3620-28TC	A1
		DGS-3620-28SC	A1
		DGS-3620-28PC	A1
		DGS-3620-52T	A1
		DGS-3620-52P	A1
Runtime: v1.00.040 Prom: v1.00.016	2011/10/7	DGS-3620-28TC	A1
		DGS-3620-28SC	A1
		DGS-3620-28PC	A1
		DGS-3620-52T	A1
		DGS-3620-52P	A1
Runtime: v2.00.016 Prom: v1.00.016	2012/1/5	DGS-3620-28TC	A1
		DGS-3620-28SC	A1
		DGS-3620-28PC	A1
		DGS-3620-52T	A1
		DGS-3620-52P	A1
Runtime: v2.50.017 Prom: v1.00.016	2013/3/25(A1) 2013/5/6(B1)	DGS-3620-28TC	A1, B1
		DGS-3620-28SC	A1, B1
		DGS-3620-28PC	A1, B1
		DGS-3620-52T	A1, B1
		DGS-3620-52P	A1, B1
Runtime: v2.60.016 Prom: v1.00.016	2013/11/4	DGS-3620-28TC	A1, B1
		DGS-3620-28SC	A1, B1
		DGS-3620-28PC	A1, B1
		DGS-3620-52T	A1, B1
		DGS-3620-52P	A1, B1
Runtime: v3.00.004 Prom: v1.00.016	2017/10/6	DGS-3620-28TC	A1, B1
		DGS-3620-28SC	A1, B1
		DGS-3620-28PC	A1, B1
		DGS-3620-52T	A1, B1
		DGS-3620-52P	A1, B1

Upgrade Instructions:

Note:
1. EI & SI features are all included in the firmware.
2. It is not necessary to upgrade PROM code.
3. Hardware version B1 supports firmware R2.50.017 and later. If downgrading to previous old versions, the switch cannot be booted up

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:

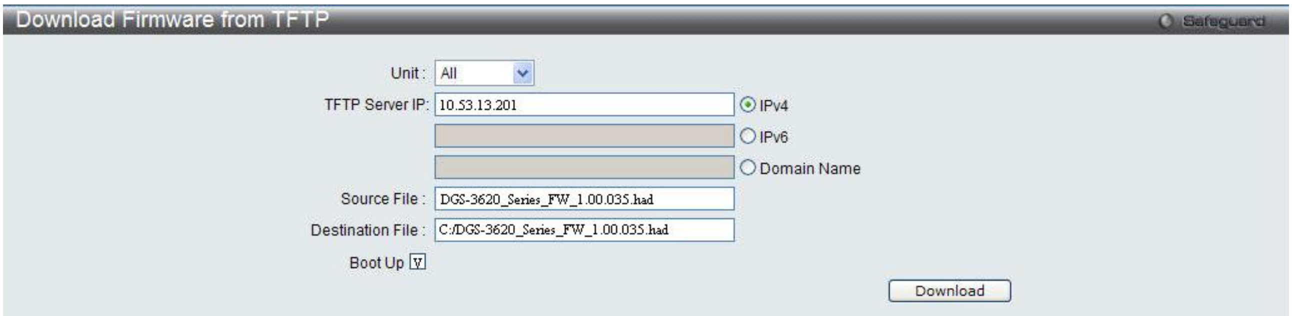
Command	Function
download [firmware_from_TFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {[unit <unit_id> | all]} {dest_file <pathname 64>}	Download firmware file from the TFTP server to the switch.
config firmware image {unit <unit_id>} <path_filename 64> boot_up	Change the boot up image file.
show boot_file	Display the information of current boot image and configuration.
reboot	Reboot the switch.

Example:

```
DGS-3620-28TC:15# download firmware_from_TFTP 10.53.13.201 src_file c:\ DGS-3620_Series_FW_1.00.035.had
dest_file   c:\ DGS-3620_Series_FW_1.00.035.had
Command: download firmware_from_TFTP 10.53.13.201 src_file c:\ DGS-3620_Series_FW_1.00.035.had dest_file
c:\ DGS-3620_Series_FW_1.00.035.had

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

DGS-3620-28TC:15# config firmware c:\ DGS-3620_Series_FW_1.00.035.had boot_up
Command: config firmware c:\ DGS-3620_Series_FW_1.00.035.had boot_up

Success.

DGS-3620-28TC:15# show boot_file
Command: show boot_file
-----------------------------------------------------
 Unit ID : 1
 Boot up firmware image : C:\DGS-3620_Series_FW_1.00.035.had
 Boot up configuration file: C:\STARTUP.CFG
 -----------------------------------------------------

DGS-3620-28TC:15# 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.
4. To update switch's firmware or configuration file, select ***Tools > Download Firmware*** from the banner.



Download Firmware from TFTP

Unit : All

TFTP Server IP: 10.53.13.201 ● IPv4

○ IPv6

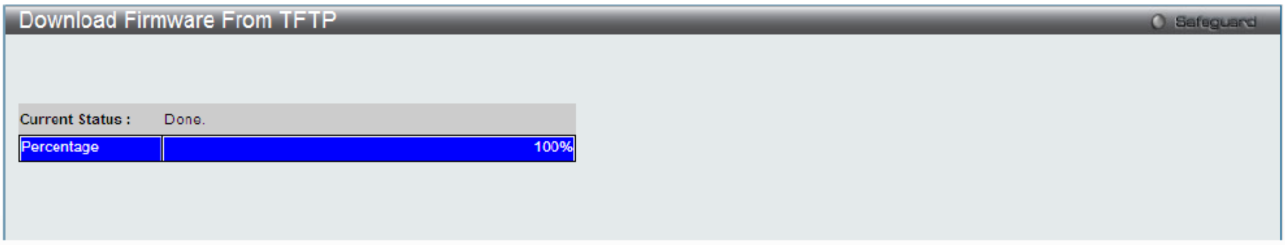
○ Domain Name

Source File : DGS-3620_Series_FW_1.00.035.had

Destination File : C:/DGS-3620_Series_FW_1.00.035.had

Boot Up ☑

5. Use the drop-down menu to select a unit for receiving the firmware. Select **All** for all units.
6. Enter the TFTP Server IP address.
7. Enter the name of the firmware file located on the TFTP server.
8. Enter the destination path and the desired file name.
9. Tick the check box to set it as a boot up file.
10. Click “***Download***” button.
11. Wait until the “Current Status” displays “Done” and the “Percentage” shows “100%”.

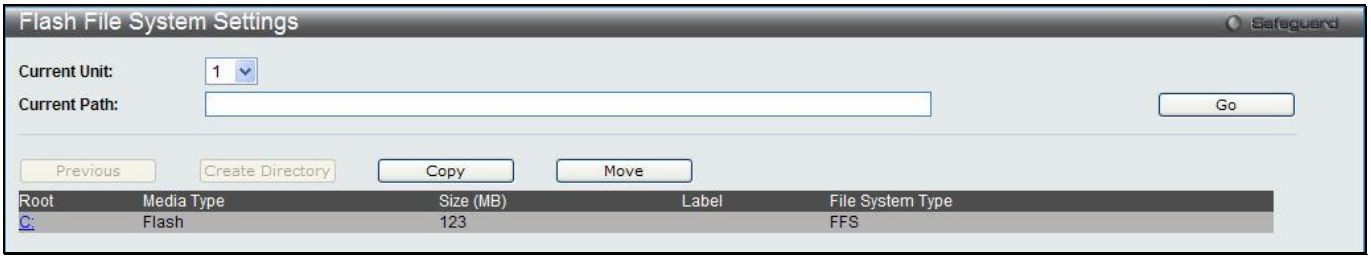


Download Firmware From TFTP

Current Status : Done.

Percentage 100%

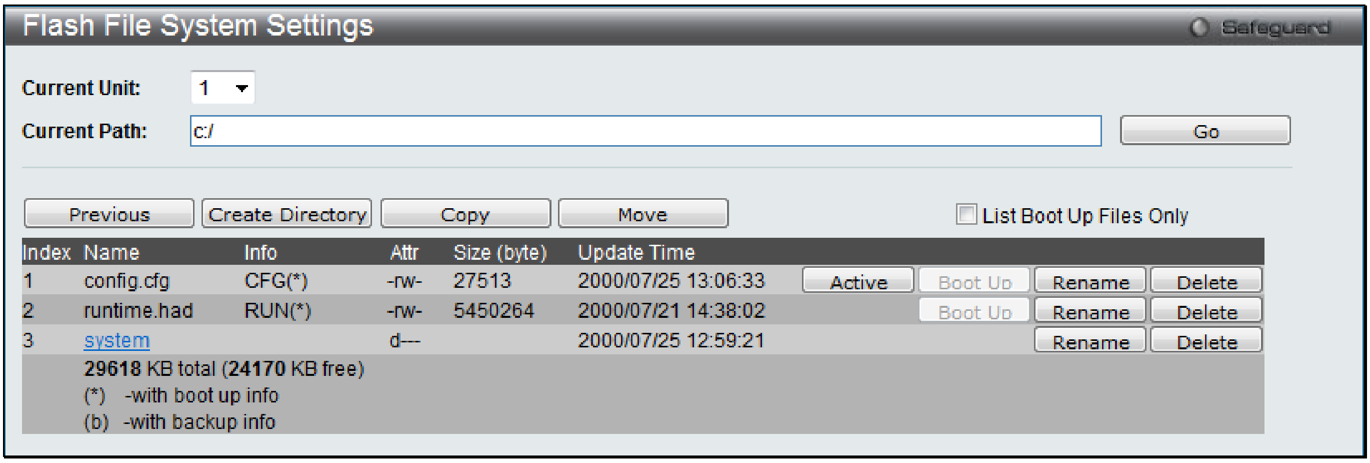
11. To select the boot up image used for next reboot, click ***Network Application > Flash File System Settings*** in the function tree and then click the ***C:*** drive name. When you see the files list, click corresponding “***Boot Up***” button to specify the firmware that will be used for next and subsequent boot up.



Current Unit: 1

Current Path:

Root	Media Type	Size (MB)	Label	File System Type
C:	Flash	123		FFS



Current Unit: 1

Current Path: c:/

Index	Name	Info	Attr	Size (byte)	Update Time
1	config.cfg	CFG(*)	-rw-	27513	2000/07/25 13:06:33
2	runtime.had	RUN(*)	-rw-	5450264	2000/07/21 14:38:02
3	system		d---		2000/07/25 12:59:21

29618 KB total (24170 KB free)
(*) -with boot up info
(b) -with backup info

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

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

DLMS Instructions:

Some D-Link switches support DLMS (D-Link License Management System) feature. With DLMS, you can upgrade your switches to more enhanced edition to get more sophisticated features.

DLMS License Activation by CLI

Command	Function
install dlms activation_code <string 25> {unit <unit_id 1-6>}	This command is used to install an activation code to activate or unlock function on the appliance.
show dlms license {unit <unit_id 1-6>}	This command is used to display license information.

Example:

1. **DGS-3620-28TC:admin#install dlms activation_code DF244A4E4BC640C6394510206**

```
Command: install dlms activation_code DF244A4E4BC640C6394510206
Success.

Please reboot the device to active the license.

DGS-3620-28TC:admin#
```

2. **DGS-3620-28TC:admin#reboot**

```
  Command: reboot
```

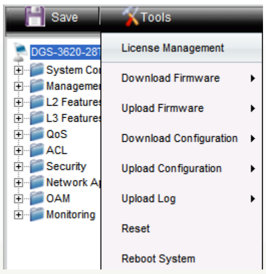
```
Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...

  Boot Procedure                                                  V1.00.016
-----------------------------------------------------------------------


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

  MAC Address    : 00-40-05-31-20-00
  H/W Version    : A1

  Please Wait, Loading V2.50.017 Runtime Image .............   100 %
  UART init ................................................   100 %
  Starting runtime image
  Device Discovery ........................................   100 %
  Configuration init ......................................   100 %
```

3. **DGS-3620-28TC:admin#show dlms license**

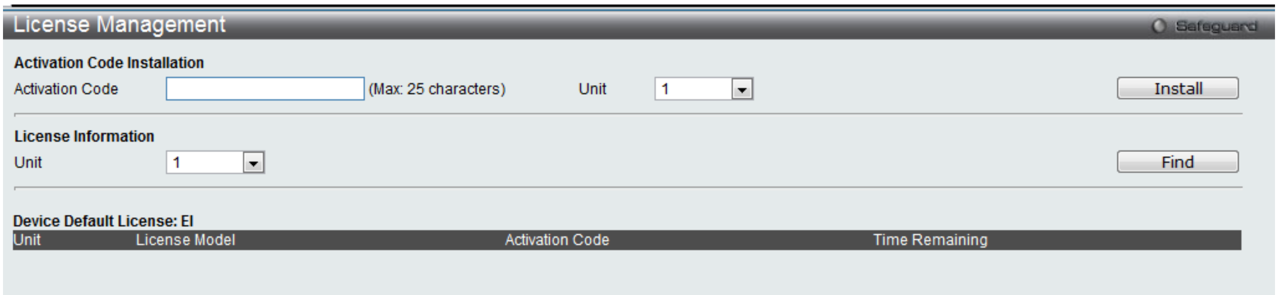
```
Command: show dlms license

Device Default License : SI

License Model                    Activation Code                  Time Remaining
---------------------------------------------------------------------------------
DGS-3620-28TC-SE-LIC             DF244A4E4BC640C6394510206        No Limited
---------------------------------------------------------------------------------
                                                                    * expired
```

DLMS License Activation by 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 ***Tool->License Management*** from the banner.



5. Enter the Activation Code and select unit of stack then click **Install** to activate the assigned switch.



License Management

Activation Code Installation

Activation Code (Max: 25 characters) Unit 1

License Information

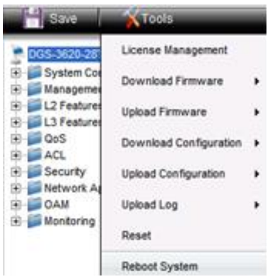
Unit 1

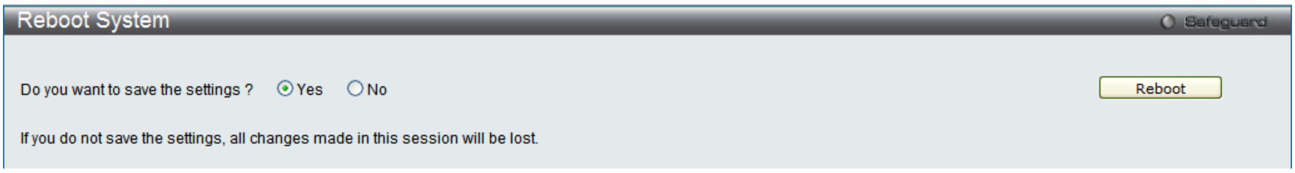
Device Default License: EI

Unit	License Model	Activation Code	Time Remaining

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

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





Reboot System

Do you want to save the settings ? ● Yes ○ No

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

New Features

Firmware Version	New Features
V1.00.035	First release, please refer to datasheet and manual for detail function supported
V1.00.038	1. Add new flash driver support – "JS28F512M29EWL". 2. Modify PoE per port default power from 7000mw to 15400mw.
V1.00.040	None
v2.00.016	1. Support D-Link License Management System(DLMS) to upgrade Standard Image (SI) to Enhance Image (EI) 2. Support external Alarm port functions 3. Supports 64 characters file name for file system 4. Enlarge PoE maximum power limit to 760W for DGS-3620-28PC 5. Support 100-FX/BX SFP Transceivers: DEM-210/211/220T/220R 6. Modify DDM shutdown default state from alarm to none 7. DSCP to CoS mapping 8. Support SNTPv6 9. Support 128 bits prefix IPv6 routing

	10. Support DEM-CB700S 10GbE SFP+ to SFP+ 7meter Direct Attach Cable
V2.50.017	1. Support null route be able to redistribute to dynamic routing protocol 2. The priority of route preference is configurable in policy based route or route table 3. Be able to disable a LACP trunk member port 4. Enlarge Super VLAN's Sub VLAN number to 128. 5. Support to display media type of SFP transceiver 6. Support UDP Helper 7. Support to send SNMP traps when LACP member port is up or down 8. Support Weighted Random Early Detection 9. Storm control supports to configure the threshold by packet types in the same port 10. Support IMPB v3.95 11. Enlarge the BGP neighbor to 20 neighbors and also support 4 byte AS number 12. Support DHCPv6 Prefix Delegation 13. Support DoS Attack Prevention 14. Support Framed-IP-Address Radius attribute 15. Support per port DHCP relay 16. The minimum granularity of bandwidth control changes to 8Kbps 17. Support unicast NLB 18. Support configurable DHCP server option 19. Support OSPF distribute list witch can limit to specific IP range 20. OSPF supports point-to-point network type 21. Modify OSPF design that one OSPF "link state update" packet be able to carry multiple "link state advertisement" entries 22. The DDM function is able to show TX/RX power 23. Be able to encrypt SNMP community name. 24. PIM supports passive mode 25. Support advanced power saving (LED Shut-off/ Port Shut-off/ System Hibernation) 26. Support DHCPv6 relay option 37 27. Support Secure FTP server for IPv4 28. Support DHCPv6 Server Screening 29. Be able to separate RADIUS accounting server from authentication server30. Support DNSv6 31. When trigger events of alarm port occur, the system is able to send alarm to external warning devices 32. IGMP authentication supports auth & accounting, auth only or accounting only modes 33. Be able to show the packet counter of STP drop/HOL drop/CoS drop 34. Support sending SNMP traps via specific port inside of all ports 35. Be able to configure SNMP UDP port number 36. DHCP Auto-configuration supports DHCP option 6, 66, 67, 150 37. Support displaying CPU port statistics 38. Support LBD v4.05 39. Support displaying more specific traffic control information for broadcast/multicast/unicast traffic types 40. Route redistribution feature supports RIPng/OSPFv3 protocols 41. TACACS+ support command accounting 42. Debug command will also display stacking port's packet statistics 43. Support Unicast Reverse Path Forwarding 44. Support selective QinQ 45. The RIP update timer downgrade to 1 sec 46. Move Cable Diagnostics function from EI to SI 47. LACP supports configuring timeout parameter 48. Y.1731 supports Loss Measurement / Delay Measurement parameter 49. Storm control feature supports sending trap/log when traffic exceeds the defined drop threshold

	50. Support 802.3az Energy-Efficient Ethernet (Hardware version B1 and later)
V2.60.016	1. Increasing stacking bandwidth to 80G (full duplex) 2. The Layer 2 function supports following new features: ● D-Link IMPB v3.96 (Support IP DHCP Snooping Limit Rate) ● VLAN-Based Mirror for Rx ● Flow-based(ACL) mirroring support egress mirroring ● Support to force 10G speed on 10G port 3. VLAN function supports following new features: ● Enlarge to 4K dynamic VLAN groups ● Support Surveillance VLAN 4. QoS function supports following new features: ● Support 802.1Qbb Priority-based Flow Control (PFC) for 10G port ● Configure Bandwidth control rate by percentage ● Support to display per CoS statistics for Tx traffic 5. The Layer 3 function supports following new features: ● RFC3484 (Default Address Selection for Internet Protocol version 6) ● BFD (Bidirectional Forwarding Detection) for OSPF/VRRP ● BGP for IPv6 ● IPv6 Stateless Address Auto Configuration (SLAAC) for host mode ● RFC3509 (Alternative Implementations of OSPF Area Border Routers) 6. The Layer 3 Multicasting function supports following new features: ● Support to display RX/TX counters of multicast protocol packet ● Support to display RP (Rendezvous Point) address in multicast group 7. Security function supports following new features: ● Support shutdown mode when the number of MAC address reaches the maximal learning limitation on the port ● SSH Public Key can associate with specific user 8. Management function supports following new features: ● IPv4/v6 FTP client ● Be able to schedule the reboot system time ● DHCP client supports option 12 ● The subtype of Port ID TLV supports MAC address or port number ● DHCP relay supports vendor 6 format ● Support to display CPU utilization per task ● Change the Cable Diagnostics usage level form Power-User level to User Level ● Support to enable or disable the Automatically Speed Downgrade feature when the highest speed link fails ● The user can configure IGMP Snooping feature to send the General Query packet or not when a port is enabled or disabled by STP
V3.00.004	1. Support enabling or disabling the MAC learning based on VLAN 2. Support displaying 802.1q queue statistics per port information 3. Support displaying LACP statistics 4. Add replace option of VLAN translation on UNI port 5. Auto Surveillance VLAN v1.4 6. Enlarge Auto Voice VLAN maximum OUIs to 10 7. Enlarge DHCP exclude address entries to 8 8. Support VLAN counters 9. Enlarge ERPS maximum rings to 26 single rings 10. Enlarge maximum manual DHCP binding entries to 250 11. MAC-based Access Control can be applied to LACP 12. NTP 13. Enlarge static route enters to 1024 14. ACL supports the action of redirect to port 15. SD card management 16. Flex Link

	17. Super VLAN for IPv6 18. TLS1.1/1.2 19. Enlarge maximum Power Saving time ranges to 20 20. Enlarge maximum DHCPv4 server excluded address ranges to 50 21. Support configuring DHCP unicast Reply packet **NOTE:** All above features ONLY are supported by CLI

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
V1.00.035	First release, please refer to datasheet for detail MIB supported	
V1.00.038	None	
V1.00.040	None	
v2.00.015	Dlms.mib	Add DLMS
	Time.mib	Add SNTPv6
	QoS.mib	Add DSCP to CoS mapping
	Equipment.mib	Support external alarm port
	PoE.mib	Enlarge PoE maximum power limit to 760W for DGS-3620-28PC
	rfc5643.mib	Update OSPFv3-MIB
V2.50.017	L3mgmtDgs3620-xx.mib	1. Support redistributing null route to dynamic routing protocol 2. Support DHCPv6 Prefix Delegation 3. Support OSPF distribution list new parameter 4. OSPF supports point-to-point network type 5. Route redistribution supports RIPng/OSPFv3 6. “RIP update timer” downgrades to 1 sec
	policyRoute.mib	The priority of route preference is configurable in policy based route or route table
	L2mgmtDgs3620-xx.mib	1. Be able to disable a LACP trunk member port 2. Support displaying media type of SFP transceiver 3. IGMP authentication supports auth_accounting, auth only or accounting only modes 4. Support displaying the packet counter of STP drop/HOL drop/CoS drop packet
	SuperVLAN.mib	Enlarge Super VLAN’s Sub VLAN number to 128.
	UDPHelper.mib	Support UDP helper
	rfc2863.mib	Support to send SNMP traps when LACP member port is up or down
	wred.mib	Support Weighted Random Early Detection
	PktStromCtrl.mib	1. Storm control supports to configure the threshold by packet types in the same port 2. Storm control feature supports sending trap/log when traffic exceeds the defined drop threshold

	IPMacBind.mib	Support IMPB v3.95
	Rfc4273.mib	Enlarge the BGP neighbor to 20 neighbors and also support 4 byte AS number
	Dosprev.mib	Support DoS Attack Prevention
	DHCPRelay.mib	Support DHCP relay per port
	QoS.mib	The minimum granularity of bandwidth control changes to 8Kbps
	NLB.mib	Support unicast NLB
	DHCPServer.mib	Support configurable DHCP server option
	DDM.mib	Be able to display TX/RX power
	Genmgmt.mib	1. Be able to encrypt SNMP community name 2. PIM supports passive mode 3. Support total learned number of ARP entries in system 4. Support sending SNMP traps via specific port inside of all ports 5. Be able to configure SNMP UDP port number
	Equipment.mib	1. Support advanced power saving (LED Shut-off/ Port Shut-off/ System Hibernation) 2. Support 802.3az Energy-Efficient Ethernet (Hardware version B1 and later)
	DHCPv6Relay.mib	Support DHCPv6 relay option 37
	SFTPServer.mib	Support Secure FTP server for IPv4
	Filter.mib	Support DHCPv6 Server Screening
	AAC.mib	1. Be able to separate RADIUS accounting server from authentication server 2. TACACS+ support command accounting
	DNSResolver.mib	DNSv6
	LBD.mib	LBD v4.05
	urpf.mib	Unicast Reverse Path Forwarding
	QinQ.mib	Selective QinQ
	ie8023ad.mib	LACP support configure timeout
	CFMExtension.mib	Y.1731 support Loss Measurement / Delay Measurement
V2.60.016	Genmgmt.mib	1. Support IPv4/v6 FTP client 2. Support to schedule the reboot system time
	L2mgmtDgs3620-xx.mib	1. Enlarge to 4K dynamic VLAN groups 2. Increasing stacking bandwidth to 80G (full duplex) 3. Support to display per CoS statistics for Tx traffic 4. Support VLAN-Based Mirror for Rx 5. Support to enable or disable the Automatically Speed Downgrade feature when the highest speed link fails 6. Support to force 10G speed on 10G port 7. The subtype of Port ID TLV supports Mac address or port number
	L3mgmtDgs3620-xx.mib	1. BFD (Bidirectional Forwarding Detection) for OSPF/VRRP 2. DHCP client supports option 12 3. Support IPv6 Stateless Address Auto Configuration (SLAAC) for host mode

	QoS.mib	Configure Bandwidth control rate by percentage
	Rspan.mib	Support VLAN-Based Mirror for Rx
	EgressACL.mib	Flow-based(ACL) mirroring support egress mirroring
	PortSecurity.mib	Support shutdown mode when the number of MAC address reaches the maximal learning limitation on the port
	IPMacBind.mib	Support D-Link IMPB v3.96 (Support IP DHCP Snooping Limit Rate)
	ssh.mib	SSH Public Key can associate with specific user
	dot1xmgmt.mib	Add 802.1X access login fail trap
	wac.mib	Add WAC access login fail trap
	SurveillanceVlan.mib	Support Surveillance VLAN
	McastSnooping.mib	The user can configure IGMP Snooping feature to send the General Query packet or not when a port is enabled or disabled by STP
	NOTE: All above features ONLY support MIB	
V3.00.004	L2mgmt.mbi	Support LACP Active Port Object
	VLANCounter.mib	VLAN Counter
	Genmgmt.mib	Support enabling or disabling the MAC learning based on VLAN
	l2mgmt.mib	Support displaying LACP statistics
	QoS.mib	Support displaying 802.1q queue statistics per port information
	qinq mib	Add replace option of VLAN translation to UNI port
	ntp.mbi	NTP
	ACL.mib	ACL supports the action of redirect to port
	SDCardMgmt.mib	SD card management
	flexlink.mib	Flex Link
	SuperVlan-MIB	Super VLAN for IPv6
	L2mgmt.mbi	Modify swL2PortSfpInfoTable’s node description
	SSL mib	TLS 1.1/1.2

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.

Firmware Version	Changes
V1.00.035	First release
V1.00.038	None
V1.00.040	None
v2.00.016	None
V2.50.017	None

V2.60.016	None
V3.00.004	None

Problem Fixed

Firmware Version	Problems
V1.00.035	First release
V1.00.038	None
V1.00.040	1. Modify CPU GPIO pin setting on DGS-3600-28SC/28TC/52T 2. Modify RTC trickle register to reduce charging time
v2.00.016	1. LAG group will be failed due to mis-matching of port configuration if power cycle in unit 2 (DI20110802000001) 2. The CPU loading of master and slave units will become 100% and make two master roles in the same stacking system. (DI20110616000011) 3. A loop condition was happened after using ERPS. After rebooted, DGS-3620 forwarded packets from RPL port whose state was blocking. (DI20110727000004) 4. Multicast packets cannot be forward after slave unit is rebooted (DI20110729000007) 5. DULD settings were lost after stacking Member unit reboot (DI20110726000012) 6. Null characters was occurred when getting the result of MIB (swERPSMgmtRAPSProtectionVlan) (DI20110726000004) 7. Console freeze when typing "show wac auth_state po*" (DI20110726000004) 8. Performance issue in WAC for IPv6 (DI20110701000011)
V2.50.017	1. After resetting configuration and executing “show config modified”, the system still displays some non-modified configuration (DUSA20110616000002) 2. Telnet session will be terminated when DGS-3620 receives unknown destination IP packets. (DI20110711000004) 3. When the packet exits service provider’s network, the switch didn’t remove the inner tag in outgoing UNI port (DRU20110919000004) 4. When enabling WAC with invalid virtual IP address, switch does not show warning message. (DI20111114000004) 5. When creating 4K VLANs, DGS-3620 will stop sending LACP/BPDU packets (DI20110616000010) 6. When over 2K JWAC authenticated clients in system and then clear all FDB entries, the switch will stop sending LACP/BPDU packets for a while (DI20110621000010) 7. When over 4K WAC authenticated clients in system and then clear all FDB entries, it will stop sending LACP/BPDU packets for a while (DI20110706000012) 8. In stacking mode, DGS-3620 will take over 50sec to delete FDB entries (DI20110621000016) 9. BGP session was terminated when DGS-3620 receives IPv6 multicast packets in 500pps. (DI20111121000006) 10. DGS-3620 will duplicate DHCP OFFER packet when receiving DHCP snooping packet with VLAN tag. (DI20111208000007) 11. The LACPDU structure doesn’t follow the standard IEEE 802.1AX-2008. (DRU20111223000001) 12. When enabling DHCPv6 snooping and multicast filter, a DHCPv6 solicit

packet will be forwarded twice. (DI20120117000007)

13. DGS-3620 didn't add (S, G) entry into PIM multicast route table for IPv6 when the interface was connected to server directly instead of DR. (DI20120106000002)
14. DHCP inform packet is returned to ingress port when flooding a DHCP packet in the VLAN (DRU20120209000002)
15. The jumbo frame can't be routed by DGS-3620 (DEUR20120119000003)
16. DGS-3620 can't reply SYN+ACK in WAC IPv6 clients after continuously process authentication and de-authentication(DI20111203000001)
17. When configuring DGS-3620's WAC feature to redirect IPv6 HTTPS traffic to specific web page, switch will redirect the traffic to incorrect authentication page. (DI20111208000010)
18. When IPv6 is enabled and be saved, it will be reset to disable again after rebooting the switch. (DRU20120402000005)
19. The status of remote MEP port displays "up" incorrectly even if the link is down. (DEUR20120408000001)
20. DGS-3620 will enter the exception mode and then auto-reboot when getting too big SNMP PDU packet (DRU20120511000004, DRU20120409000001)
21. When DGS-3620 implements inter-VLAN routing, the ingress packets without setting 802.1p priority will be modified to priority 5 in egress. (DRU20120516000002)
22. The loopback interface was not written into hardware table when disabling system interface (DRU20120530000003)
23. After receiving the last authenticated entry via TACACS+, DGS-3620 can't time out telnet session. (DEUR20120611000001, DRU20120710000005)
24. When routing DHCP packet to next hop and the ARP entry of next hop is not in ARP table, DGS-3620 can't send ARP request actively and forward DHCP packets (DRU20120628000002)
25. After installing the activation code, it still displays Standard Image instead of Enhanced Image when executing "show switch" command(DGC20120712000001)
26. When DGS-3620 is RP role in PIM-SM, it can't keep register message (DRU20120712000006)
27. When leaving one IGMP group and re-joining this group again, it join action will be delayed around 1 minute (DRU20120626000002)
28. When executing download/upload file script, it will cause the system memory pool exhausted. (DRU20120402000004)
29. DGS-3620 detects the loop incorrectly in LBD VLAN based mode when connects ports in different VLANs. (DI20120718000002)
30. DGS-3620 receives multiple multicast groups, the switch will send incorrect IGMP report packet to server, which will work fine when receiving signal multicast group(DUSA20120719000002)
31. If the switch's system interfaces and management interface connect to TFTP server, download firmware will be failed. (DI20120914000006)
32. DGS-3620 will hang up when enabling BGP (DRU20120924000004)
33. When CPU utilization was high, OAM frame will be stopped (DI20110728000011)
34. IPv6 multicast stream was not transmitted by PIM6 after the reboot (DI20110831000006)
35. In stacking, DGS-3620 will still forward CFM frames from ERPS blocking port after rebooting the backup master unit. (DI20110908000011)
36. After disconnecting a cable from a master unit's LACP port DGS-3620 cannot forward packet to CPU (DI20110909000001)

	37. After master unit of a stack was powered off, the slave unit’s RPL port is still in block state instead of changing to forward state (DI20110909000002) 38. When DGS-3620 receives IPv6 multicast packet(LLNMR/SSDP) by 1000pps, DGS-3620 will drop BGP keep-alive packets and terminate BGP session (DI20110905000009) 39. User cannot change the port speed to 100 full via Web-UI (DRU20110915000007) 40. DGS-3620 will auto reboot when executing SSH attack tool(rubyinstaller) (DI20121012000004) 41 DGS-3620 does not forward DHCP packets if interface is disabled and DHCP relay is enabled (DRU20121025000011) 42 In stacking, when Voice VLAN is enabled first and then assigns VLAN member ports form slave unit, DGS-3620 will not learn MAC addresses from those VLAN member ports (DEUR20121220000001)
V2.60.017	1. The user login to DGS-3620 via SSH firstly, then telnet to other device from current DGS-3620, the CPU utilization will raise to 100% (DRU20130527000008) 2. When setting up time zone parameter, the time of syslog message does not apply the change of time zone (DRU20130313000003) 3. The client cannot renew IP address when enabling DHCP relay which has configured VRRP (DI20130305000002) 4. The customer uses SNMPWALK tool to show DGS-3620 ARP table which has many ARP enters, DGS-3620 CPU utilization will raise to 93%~96% (DUSA20130330000001) 5. When login switch via RADIUS, the user executes “enable admin” command and then “show log” command, the username of syslog is Anonymous instead of correct user name (DRU20130410000006) 6. When user enables VRRP and then enable DHCP Relay feature in DGS-3620 , if a client sends a unicast DHCP request packet to DHCP server, the DHCP server will receive two DHCP request packets (DI20130325000003) (DI20130419000006) 7. If LACP master port is not a flooding port, DGS-3620 cannot forward DHCP packets (DI20130419000006) 8. When enabling IMPB and DHCP snooping, the user configures DHCP Snooping’s maximum entry to 1 entry only. The switch will be learned 2 DHCP clients (DRU20130523000006) 9. In stack mode, maser switch is powered off. The user access to the backup master switch using SSH, it should be login admin level, however it login user mode (login#) (DI20130603000002) 10. After querying "swPimNeighborExpiryTime" OID under PIM-SM MIB tree, DGS-3620 will enter the exception mode (DRU20130618000003) 11. In stack mode, when DGS-3620 receives high rate (1000pps) of IPv6 multicast packets, STP function is unstable (DI20130618000006) 12. DGS-3620 cannot resolve DNS records, which contained CNAME associates multiple A records (DI20130612000001) 13. When uploading configuration/log to TFTP or downloading firmware/configuration from TFTP, DGS-3620 cannot resolve DNS AAAA records (DI20130612000001) 14. The client of Sub VLAN cannot receive IP address from DGS-3620 when DHCP server is in Super VLAN (DI20130611000002) 15. iBGP session would be terminated when enabling PIMv4 or PIMv6 with large amount of multicast traffics be forwarded (DI20130619000008) (DI20130621000003) 16. DGS-3620 doesn’t send PIM Hello or Bootstrap message after enabling CFM (DI20130116000001) 17. When MAC address of next hop is changed, ND entry cannot be

	auto-updated. It will fail to ping global IPv6 address of next hop (DEUR20121119000001) 18. When Private VLAN is configured in DGS-3620 stack, the client still can communicate with other client in different VLAN. However, If the client is moved to different switch and still in the same VLAN ID, the client will not able to communicate with other client in different VLAN (DI20130123000003) 19. When DHCP relay is enabled, DGS-3620 cannot forward DHCP packet if layer 3 interface is disabled. Actually, the DHCP relay should be worked even layer 3 interface is disable (DRU20130218000004) 20. When DHCP relay is enabled, DGS-3620 cannot forward DHCP packet if DHCP server and DHCP client are different subnet (DRU20130218000004) 21. MacBook OS 10.7 can be net-booted via DGS-3620, but the previous MacBook OS version cannot be net-booted (DUSA20130410000002) 22. If DHCP Relay is enabled, the QinQ VLAN Translation works abnormally (DEUR20130515000004) 23. The display is very slow when executing the command of “show config effective" and "show config current_config" via SSH (DI20130704000006) 24. If the Multicast filtering mode is configured as “filter_unregistered”, the IPv6 multicast stream cannot be flooded to same VLAN ports correctly (DI20130711000008) 25. BGP is configured. Sometimes, DGS-3620 doesn’t apply BGP prefix in the packet(DRU20130708000004) 26. The webpages of MAC-based Access Control Port Setting list/ MAC-based Access Control Authentication State list/ MAC address table are unfriendly (DEUR20130628000002) 27. When PIM-SM interface is changed, the old passive interface is not equal to new passive interface because PIM-SM’s passive interface doesn’t set the value. DGS-3620 deletes all neighbours and then system will crash because the switch cannot find any neighbours when sending PIM Join/Prune message (DI20130624000004) 28. When upgrading the firmware, customer cannot access to DGS-3620 via out-of-band interface using SSH while WebUI has no such issue (DEUR20130715000008) 29. If DGS-3620 receives multicast packets which cannot match IP multicast routing table inside the switch, the CPU’s utilization will remain high (DI20130712000002)

V3.00.004	1. Fixed the issue that the Tx/Rx state of manually configured trunk interface's active port is inconsistent when configuring LACP's port mode (DI20140512000009) (DI20140704000005) 2. Fixed the issue that the switch doesn't update the SIM topology information via Web UI (DEUR20140725000002) 3. Fixed the issue that average temperature calculation is incorrect via SNMP (DEUR20140708000001) 4. Fixed the issue that the switch will enter into system exception status when typing 108 characters (DI20140725000002) 5. Fixed the issue that the status of OSPFv3 protocol is not the same between the stacking master and the members after the switch is rebooted (DI20140805000005) 6. Fixed the issues that DLMS license is incorrect on stacking member (DUSA20140828000001) 7. Fixed the issue that there are a lot of oversized packets on the stack port when Jumbo Frame is enabled (DEUR20141008000001) 8. Fixed the issue that the switch's log will display abnormal status when continually plugs/ unplugs DEM-431XT-DD transceiver (DUSA20150305000002) 9. Fixed the issue that when typing "show config modified" command and enabling ND Snooping, the switch will miss the output of DHCPv6 server related configurations (DEUR20141007000001) 10. Fixed the issue that the CPU utilization will be high if the switch received a log of IPv6 LLA packets (DIP= FE80:xxxx…) (DI20141021000003) 11. Fixed the issue that switch displayed "system lock by other session" message when typing "sh config", "save", or "reboot" commands via telnet (DI20141217000002) 12. Fixed the issue that switch will reboot due to CPU exception if switch's web server received an http packet without User-Agent field (DRU20150224000005) 13. Fixed the issue that DHCP relay is not working when DHCP server is located in different network (DRU20130812000004) (DUSA20140716000002) 14. Fixed the issue that switch's CPU counter treated all UDP packets as UDP helper packets although the UDP helper function was disabled (DRU20130822000001) 15. Fixed the issue that sometimes the stack status is not stable when "Force Master Role" is enabled and then the slave units are occasionally rebooted. (DEUR20130806000002) 16. Fixed the issue that sometimes L3 interfaces were not work but L2 features worked well in stacking's member switches. (DEUR20130916000007) 17. When switch enabled sFlow and kept on receiving multicast packets (500pps) from sFlow collector, stacking master's console will be frozen (DI20130913000009) 18. Fixed the issue that DGS-3620 will sometimes suddenly rebooted (DI20131031000005) 19. Fixed the issue that ACL rule is incorrect after configuring PBR rules or rebooting the switch(DRU20131024000004) 20. Fixed the issue that the switch will advertise the OSPFv3's route information even if the related physical interface is down. (DI20131107000009) 21. Fixed the issue that switch did not receive link partner's LACP packet but still sent packets with Expired Flag when stacking topology changed from Ring to Chain (DI20131018000006) 22. Fixed the issue that LACP was expired incorrectly when DGS-3620 had

	learned 5000 entries via OSPFv3 routing protocol. (DI20131018000004) 23. Java applet does not include new D-Link certification (DEUR20140416000009) 24. When configured switch with following command lines, “create snmp view ViewACL 1 view_type excluded”, “create snmp community ViewACL view ViewACL read_only”, and executed the “snmpwalk -v2c -c ViewACL <IP address>” command in laptop, the switch will crash. (DRU20140515000002) 25. After executing “config dhcp_relay unicast disable”, the command only could be displayed by “show config current_config” command, but cannot be displayed by “show config modified begin "dhcp_r"” or “show config effective begin "dhcp_r"". (DI20140106000004) 26. Fixed the issue that user is still in Guest VLAN even if passing the 802.1X authentication with Juniper UAC server (DLA20140117000004) 27. Fixed the issue that the FDB table learned incorrect VRRP Virtual MAC address when Stacking Master rebooted (DI20140107000013) 28. Fixed the issue that Voice VLAN’s port is not based on Voice VLAN rules to forward traffic when Voice VLAN and DHCP relay are enabled (DEUR20140207000006) 29. Fixed the issue that the sFlow sample pool should be the total number of packets that could have been sampled, instead of the number of the sampled packets. (DI20140210000004) 30. Fixed the issue that the switch does not display “enable address binding dhcp_snoop” when typing the “show config modified” (DEUR20140225000005) 31. Fixed the issue that switch will incorrectly age out PPPoE client’s MAC address even there were traffic coming from that client. (DRU20140212000004) 32. Fixed the issue that traffic forward is incorrect when enabling PBR and default route both (DI20140403000003) 33. Fixed the issue that the port settings are not applied when upgrading firmware version from 2.00 to 2.61 (DRU20140423000001) 34. Fixed the issue that switch will automatically reboot due to the CPU exception (DI20140428000001) 35. Fixed the issue that user cannot pass 802.1X authentication when connecting to the stacking slave unit (DEUR20130603000005) 36. Fixed the issue that the switch still sent storm control event even if the threshold did not exceed the predefined amount. (DRU20140307000001) 37. Fixed the issue that the switch will crash when 802.1X client sent user name with more than 128 bytes length to switch (DEUR20140205000003) 38. Fixed the issue that switch is not forwarded ARP reply from client to DHCP server and lost ping packet when IMPB and LACP are configured (DEUR20140221000001) 39. Fixed the issue that switch didn’t create an ND Snooping entry when Windows 7 client successfully got an IP address from DHCPv6 server (DEUR20140227000007) 40. Fixed the issue that the switch has a lot of oversized packets on 10G ports when Jumbo Frame is enabled (DRU20140827000008) 41. Fixed the issue that the fiber port will link down and changed to Error-Disable status when plugging/ unplugging or disabling/ enabling 3rd party’s transceiver (DLA20141028000003) 42. Fixed the issue that different port has individual MAC address. However, the result of SNMP query will be the same MAC address (DGC20141022000004)

43. Fixed the issue that CPU utilization is high when receiving a log of IPv6 Link-Local addresses (DI20141021000003)
44. Fixed the issue that Web UI cannot create ACL entry when client is Windows 8 with IE 10 (DI20140925000004)
45. Fixed the issue that switch doesn’t update MAC address on forwarding port when ERPS is changed (DRU20140430000004)
46. Fixed the issue that when typing show config modified command line in console, the output of SNTP secondary IP address is incorrect (DRU20150205000003)
47. Fixed the issue that an error occurred when using SNMPWALK to query OID 1.3.6.1.2.1.83.1.1.4.1.2 (DRU20141210000002)
48. Fixed the issue that homepage of Web UI is missing login timeout information. (DI20161028000003)
49. Fixed the issue that switch will silently reboot (DRU20150728000002)
50. Fixed the issue that the display of ifName is incorrect (DRU20151027000007)
51. Fixed the issue that OSPFv3 LSAs are auto deleted when OSPFv3 neighbour is in Exchange status (DI20150403000001)
52. Fixed the issue that user cannot configure BGP peer activity via SNMP (DRU20160824000001)
53. Fixed the issue that Subnet VLAN configuration cannot be saved when Subnet VLAN is created by Web UI (DEUR20160830000008)
54. Fixed the issue that DGS-3620 should not drop double tagged IGMP packets when enabling QinQ and IGMP Snooping (DRU20160811000005)
55. Fixed the issue that the log will display abnormal status when plugging/ unplugging SFP transceiver for many times (IMA20160805000001)
56. Fixed the issue that DGS-3620 didn’t reply the last TFTP Block packet to D-View 7 when restoring configuration via D-View 7 (DI20160721000002)
57. Fixed the issue that switch will silently reboot because the IPv6 packet’s checksum is incorrect (DRU20160624000003)
58. Fixed the issue that DGS-3620 displays incorrect information when typing show fdb v and then pressing the Tab key (DRU20160617000001)
59. Fixed the issue that DGS-3620 SFP port will link down suddenly (DI20140701000001)
60. Fixed the issue that the stacking is failed and displayed “allocate memory fail in stk_if_dis_option_check" message. (DI20150626000006)
61. Fixed the issue that DGS-3620 will stop forwarding traffics in minutes when plugging a specific faulty SFP transceiver (DEUR20131112000007)
62. Fixed the issue that LACP member port on stacking slave unit’s combo ports cannot be an active port (DI20131225000002)
63. Fixed the issue that the switch cannot create the ND snooping entry with Windows 7 client (DEUR20140312000003)
64. Fixed the issue that Web UI format is incorrect when configuring network application via IE 10 (DGC20140206000003)
65. Fixed the issue that some configurations are lost on Backup Master role after stacked Master role is shutdown (DI20150116000001)

* D-Link tracking number is enclosed in ()

Known Issues

Firmware Version	Issues	Workaround
V1.00.035	None	
V1.00.038	None	
V1.00.040	None	
v2.00.016	None	
V2.50.017	None	
V2.60.016	CVE-ID: CVE-2013-0149 Due to the ambiguous definition in OSPF protocol as specified in RFC2328, the attacker can send a false Link State Advertisement (LSA) which will evade the fight-back mechanism so that the LSA may be accepted and propagated by a “genuine” router on the network.	1. Enable MD5 authentication for OSPF 2. Enable OSPF Passive Interface to stop sending or receiving routing table update on interfaces that do not participate in OSPF 3. Enable MAC-based Access Control (MAC) to authenticate devices before they are able to communicate with the network
V3.00.004	None	

Related Documentation

- DGS-3620 Series Web UI Reference Guide Release 2.60
- DGS-3620 Series CLI Reference Guide Release 3.00
- DGS-3620_Series_HW Installation Guide_v2.60