Firmware Version: V1.16.002
Prom Code Version: V1.00.006
Published: Jan. 28, 2021

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 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: v1.16.002 PROM: v1.00.006	28-Jan-21	DGS-3130-30TS	A1, A2
		DGS-3130-30S DGS-3130-30PS DGS-3130-54TS DGS-3130-54S DGS-3130-54PS	A1
Runtime: v1.10.057 PROM: v1.00.006	18-Dec-19	DGS-3130-30TS DGS-3130-30S DGS-3130-30PS DGS-3130-54TS DGS-3130-54S DGS-3130-54PS	A1
Runtime: v1.10.B032 PROM: v1.00.006	31-Jul-19	DGS-3130-30TS DGS-3130-30S DGS-3130-30PS DGS-3130-54TS DGS-3130-54S DGS-3130-54PS	A1
Runtime: v1.01.B027 PROM: v1.00.006	18-Sep-18	DGS-3130-30TS DGS-3130-30S DGS-3130-30PS DGS-3130-54TS DGS-3130-54S DGS-3130-54PS	A1
Runtime: v1.01.026 PROM: v1.00.005	31-Jul-18	DGS-3130-30TS DGS-3130-30S DGS-3130-30PS DGS-3130-54TS DGS-3130-54S DGS-3130-54PS	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
copy {tftp: [//*LOCATION*/*SOURCE-URL***]}** *DESTINATION-URL*	Download firmware file from the TFTP server to the switch.
boot image URL	Change the boot up image file.
show version	Display Switch information.
reboot	Reboot the switch.

Example:

```
Switch#copy tftp: //10.90.90.100/DGS3130_RUN_1.10.057.img flash:
DGS3130_RUN_1.10.057.img
Address of remote host [10.90.90.100]?
Source filename [DGS3130_RUN_1.10.057.img]?
Destination filename [DGS3130_RUN_1.10.057.img]?
Accessing tftp://10.90.90.100/DGS3130_RUN_1.10.057.img...
Transmission start...
Transmission finished, file length 26737892 bytes.
Please wait, programming flash.............. Done.

Switch#
```

```
1.   Switch# configure terminal
     Switch(config)# boot image c:/DGS3130_RUN_1.10.057.img
     Copy in progress...........................100%
```

```
2.  Switch#show version

    Device MAC Address: 74:DA:D1:88:C9:00
    System MAC Address: 74:DA:D1:88:C9:01

    Unit ID  Module Name        Versions
    -------  -----------------  --------------------
    1        DGS-3130-54PS      H/W:A1
                                Bootloader:1.00.006
                                Runtime:1.10.057

3.  Switch# reboot
    Are you sure you want to proceed with the system reboot? (y/n) y
```

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 switch's firmware or configuration file, select **Tools > Firmware Upgrade & Backup** from the banner.
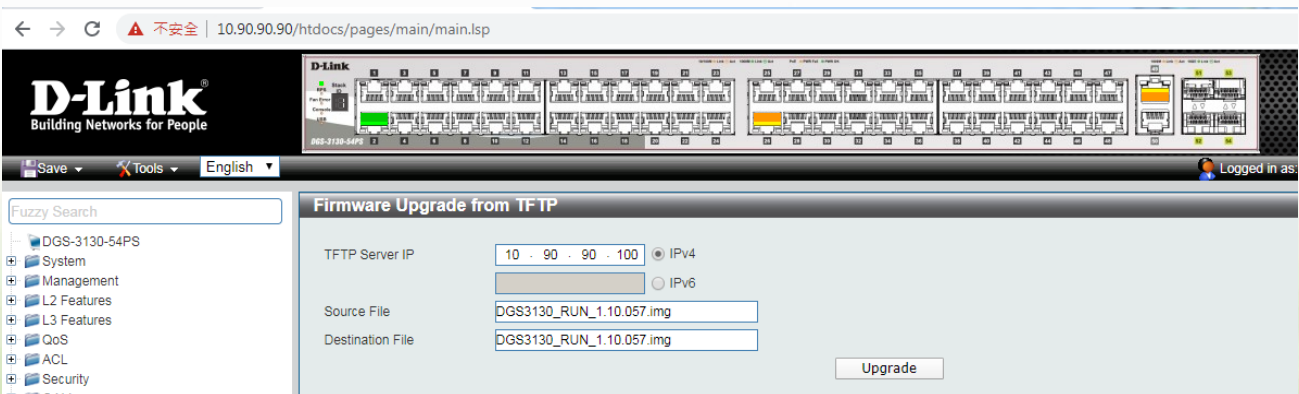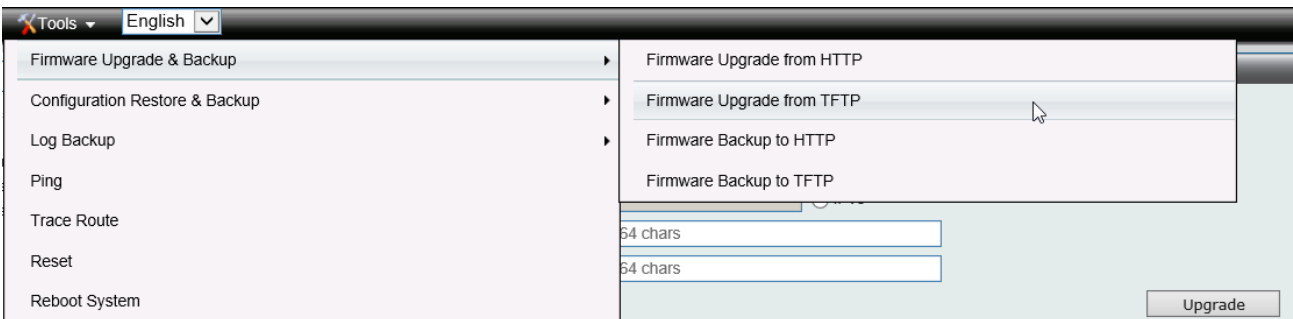


5. Enter the TFTP Server IP address.

6. Enter the location and name of the Source File on the TFTP server (ex. DGS3130_RUN_1.10.B032.img) and name of the destination file in the switch.
7. Click "**Upgrade**" button.
8. Wait until the "Current Status" reaches 100% and shows "Done".
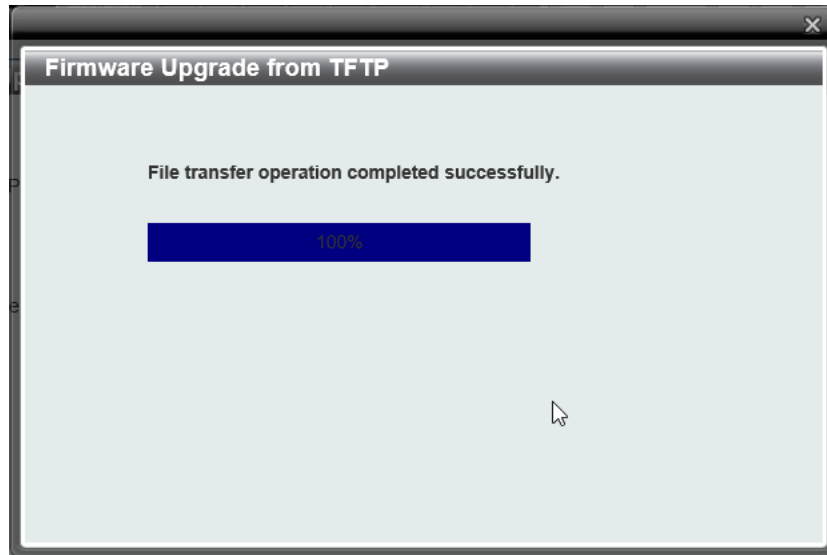
9. To select the boot up image used for next reboot, click "**Management > File System**" in the function tree. Enter the Current Path string and click the Go button or click the C: to enter "File System" window.
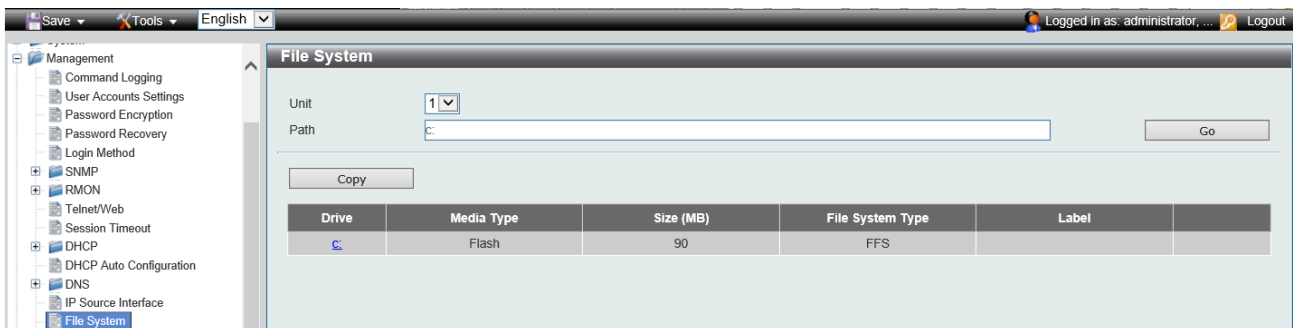
10. Click corresponding "**Boot UP**" button to specify the firmware that will be used for next and subsequent boot up.
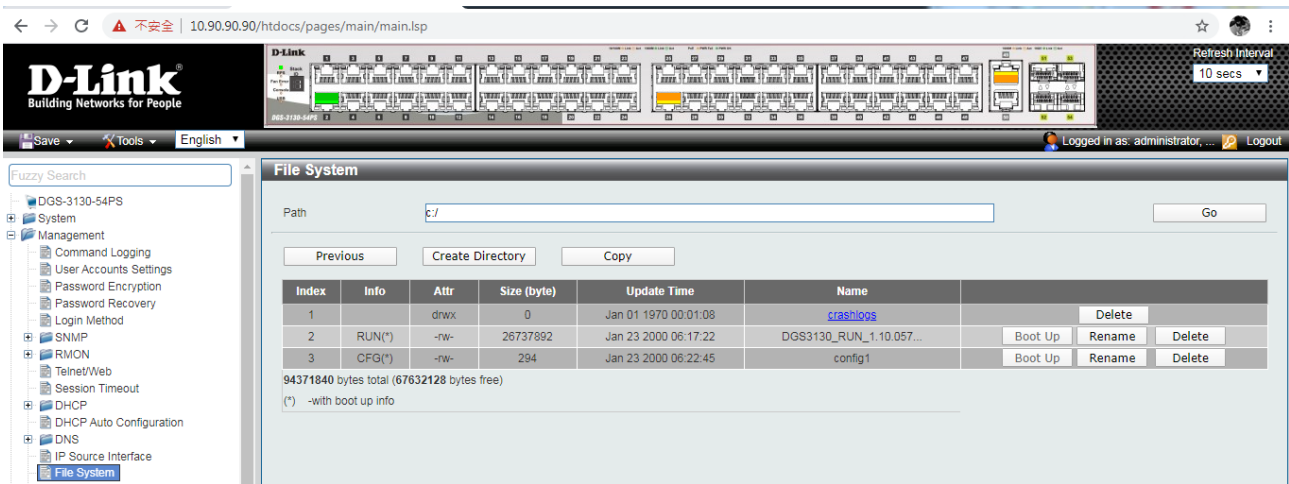
11. To reboot the switch, select **Tools > Reboot System** from the banner.
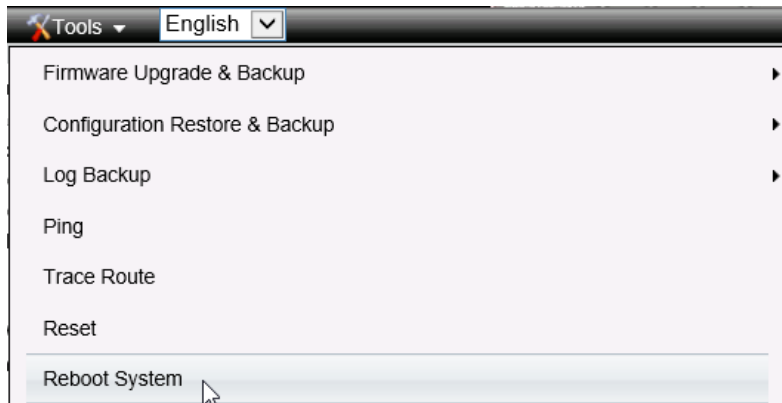
12. Select "**Yes"** and click "**Reboot**" button to reboot the switch.

New Features:

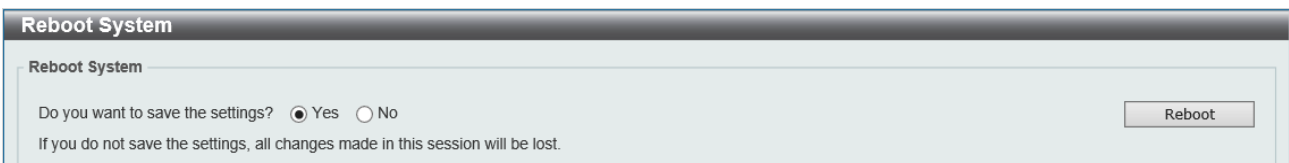| Firmware Version	New Features

V1.16.002	1. Supports RADIUS Change of Authorization (CoA).
	
	2. Supports Banner command on CLI.
	
	3. Supports Compound Authentication.
	
	4. Supports VLAN Counter.
	
	5. VLAN Translation Enhancement on UNI Port which will:
	   - UNI ingress: add SVID and replace CVID
	   - UNI egress: strip SVID and replace CVID
	
	6. Supports IGMP/MLD Snooping proxy-reporting.
	
	7. Supports 802.1p Queue Statistics.
	
	8. Web GUI supports configuring IGMP and PIM-SM.
	
	9. Supports VRRPv3 (IPv6).
	
	10. Supports sending trap or keeping log when stacking topology changed.
	
	11. Allowing user to configure multiple DHCP binding entries in a DHCP pool.
	
	12. The Web GUI's DHCP Snooping Binding Entry feature supports searching and deleting one or more binding entries.
	
	13. Improving the display format of "Current Link Duration" when user tries to use CLI showing the detailed information of an interface.
	
	14. The "show running-config" command supports "effective" or "all" parameters.
	
	15. Enhancing the IGMP authentication and accounting feature which allows switch to locally grant access to any multicast group on behalf of the RADIUS sever, but still sending Accounting-Start and Accounting-Stop to RADIUS server.
	
	16. The Web GUI supports CPU Port Utilization displaying.
	
	17. The Web GUI is able to support multiple MAC address input formats.
	
	18. Supports Multi-Process RSTP.
	
	19. User can enable DiffServ and ACL on the same interface in the same direction now.
	
	20. The IP Interface enlarges to 128 and ARP enlarges to 4K.
	
	21. User can configure different IP address as the RADIUS attribute 4 address inside the RADIUS packets.
	
	22. Supports Interface Description feature.
	
	23. No matter the IGMP Snooping Querier is enabled or not, the Querier IP address will be displayed if IGMP Snooping is enabled.
	
	24. The debug feature now supports "debug show cpu counter" command.

25. The "show interface" command now can display historical utilization of CPU/ Memory/ Interfaces/ Interfaces Counters.

26. Enhancing the DoS Prevention feature to support both log and trap.

27. For the Blat-Attack type of DoS attack, user can decide if TCP or UDP packet should be dropped now.

28. Supports IGMP Snooping Authentication.

29. The IPv6 Static Route now supports Primary and Secondary route parameters.

30. Supports half duplex for 10M/100M speed.

31. Enhancing the Dropped Packet Counter to support following counters:

   - HoL Drop

   - CoS Drop

   - STP Drop

32. Supports VLAN Wizard.

33. Supports HoL Prevention.

34. Removes the support of DHCP Server Port-Based Address Allocation feature.

V1.10.057	1. Modifing the max. VLAN support entry to 64 for both IGMP Snooping and MLD Snooping.

1. Modifing the max. VLAN support entry to 64 for both IGMP Snooping and MLD Snooping.

2. Supports L3 control packet filtering feature.

3. Supports the modification of sFlow agent's IP address.

4. User can overwrite the boot image from Web GUI directly.

5. Adding the progress bar when setting boot image from Web GUI.

6. RADIUS supports PAP.

7. Supports configuring Data Glean feature from Web GUI and SNMP now.

8. Supports turning on or off the status of ACL VLAN access-map.

9. Supports configuring Ping's frequency.

10. Supports PD Alive.

11. The Web ACL Configuration Wizard supports configuring VLAN Range and Extended Expert ACL features.

12. The Web GUI supports configuring Extended Expert ACL feature.

13. Supports Route Map.

14. Supports Policy Based Routing (PBR).

15. Supports IGMP and MLD features.

16. Supports DULD.

17. Supports 802.1ag CFM.

18. Supports Y.1731 CFM.

19. Supports ERPS multi-ring or sub-ring.

	20. Ctrl-C hot key will stop CLI displaying continuous output.
	
	21. Supports per port DHCP local relay.
	
	22. Supports DHCPv6 Option 18.
	
	23. Supports DHCP Auto-Configuration.
	
	24. Supports DHCP Option 82 – Circuit ID.
	
	25. Supports RFC 4292 MIB.
	
	26. Supports DEM-410T transceiver.
	
	27. Supports IPv4/IPv6 Server Screen.
	
	28. Supports limited IPv4 PIM-SM
	
	    - PIM-SM and Stacking-Lite are mutually exclusive.
	
	    - IGMP will be enabled by default

V1.01.B027	Improve Stacking Lite which supports pre-configure capability. - If a switch in the stack leaving, user still can configure switch with that switch's ID. Once the switch backs to the stack, configuration will take effect immediately.
V1.01.026	First Release

Changes of MIB:

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

Firmware Version	MIB File	New Features
V1.16.002	1. DLINKES-STACK-MIB	1. Supports following objects: - esStackMIBNotifications - esStackTPChangeNotification - esStackTrapStateEnabled - esStackNotificationInfo - esStackNotifyInfoBoxId - esStackNotifyInfoTopologyType - esStackNotifGroup
	2. RFC 4363 P-BRIDGE MIB	1. Supports dot1qStaticUnicastTable 2. Supports dot1qStaticMulticastTable
	3. DLINKES-STORM-CTRL-MIB	1. Changes "esStormCtrlPollingInterval" range to 5 ~ 600.
	4. DLINKES-L2PT-MIB	1. Supports esL2ptTunnelingMac
	5. DLINKES-STP-EXT-MIB	1. Supports following objects: - esStpExtPortMptTreeID - esStpExtMptTreeTable - esStpExtMptTreeIeee8021InfoTable - esStpExtPortLinkType
	6. DLINKES-MGMD-SNOOPING-MIB	1. Supports following objects: - esMgmdSnpIfQuerierExpiryTime - esMgmdSnpIfQuerier - esMgmdSnpIfQuerierExpiryTime - esMgmdSnpPortIfAuthState - esMgmdSnpIfLimit - esMgmdSnpAccGrp 2. Changes esMgmdSnpIfLimitValue to 1 ~ 1024. 3. Adds limitation 1~100 to esMgmdSnpPortIfRateLimit object.
	7. RFC4836 MAU-MIB	1. Updates IfMauDefaultType to support 100BASE-TX Full and Half Duplex. 2. Updates ifMauAutoNegCapAdvertisedBits to support 10BASE-T and 100BASE-TX.
	8. DLINKES-DOS-PREVENT-MIB	1. Add esDoSPrevBlatAttackPktType object to support Blat-Type TCP and UDP.

	9. DLINKSW-CONTROLLER-MIB	1. Supports dHeadOfLinePrevention object.
	10. DLINKES-ACL-MIB	1. Supports following objects: - esAclMacAccessListCounterEnabled - esAclMacAccessListClearStatAction - esAclIpAccessListCounterEnabled - esAclIpAccessListClearStatAction - esAclIPv6AccessListCounterEnabled - esAclIPv6AccessListClearStatAction - esAclExpertAccessListCounterEnabled - esAclExpertAccessListClearStatAction - esAclAccessGroupCounterTable
	11. DLINKES-IF-COUNTER-MIB	1. Supports following objects: - esIfCounterRxDrop - esIfCounterTxDrop
V1.10.057	1. Removing dlinkEsSFlowMIB and add dlinkSwSFlowMIB 2. dlinkSwSFlowMIB adds new objects: - dSFlowCfgAgentAddressIPv4 - dSFlowCfgAgentAddressIPv6 3. Adding following new MIBs - DLINKES-IPV6-SNOOPING-MIB - DLINKES-PACKET-MONITOR-MIB - DLINKES-IP-EXT-MIB - DLINKES-STACK-MIB - MGMD-STD-MIB - DLINKSW-IP-ROUTING-MIB - RFC 4292-IP Forwarding Table MIB 4. Removing following MIBs - DLINKSW-MGMD-EXT-MIB - DLINKSW-MGMD-PROXY-MIB	1. dlinkSwSFlowMIB supports sFlow feature. 2. DLINKES-IPV6-SNOOPING-MIB supports IPv6 Snooping feature. 3. DLINKES-PACKET-MONITOR-MIB supports Port Mirroring feature. 4. DLINKES-IP-EXT-MIB supports IP Interface feature. 5. DLINKES-STACK-MIB supports Stacking feature. 6. MGMD-STD-MIB supports IGMP feature. 7. DLINKSW-IP-ROUTING-MIB supports IP Routing feature. 8. RFC 4292-IP Forwarding Table MIB supports IP Forwarding Table configuration.
V1.01.B027	No change	
V1.01.026	First Release	

dlink green

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
V1.16.002	No change
V1.10.057	No change
V1.01.B027	No change
V1.01.026	First Release

Problem Fixed:

Firmware Version	Problems Fixed
V1.16.002	1. Fixed the issue that user cannot use snmpset command to configure switch. (DRU20201029000002) 2. Fixed the issue that the rate limit configuration sometimes would disappear after rebooting the switch. (DEUR20200814000002) 3. Fixed the issue that if switch enabled both Q-in-Q and RSTP features, DGS-3130 cannot see the root bridge information. (DRU20200813000002) 4. Fixed the issue that the LLDP configuration would disappear after rebooting the switch. (DEUR20200817000001) 5. Fixed the issue that switch cannot replace CVID to correct one when packets came from NNI to UNI port. (DEUR20200406000005) 6. Fixed the issue that ACL and DiffServ cannot be enabled at the same time. (DRU20200420000001) 7. Fixed the issue that sometimes the default route would disappear and user had to reboot the switch to back to normal. (DEUR20200519000004) 8. Fixed the issue that user cannot login the switch via SSH session. (DRU20200610000003) 9. Fixed the issue that if user configured DGS-3130's fiber port with speed 100M, the actual link speed would be 1000M but not 100M. (DEUR20200309000002) 10. Fixed the issue that both port speed and description cannot be configured by Web GUI. (DEUR20200302000003) 11. Fixed the issue that when user configured 802.1X with control-direction parameter, all packets which include DHCP packet would be dropped. (DEUR20200417000001) 12. Fixed the issue that the authenticated MAC address number did not match the configured entry number when user enabled MAC Authentication on switch. (DI20200403000005, DI20200508000003) 13. Fixed the issue that the strom control feature cannot be configured by SNMP protocol. (DRU20200519000003) 14. Fixed the issue that user cannot use SNMP protocol to configure Spanning Tree Link Type feature with point-to-point parameter. (DRU20200519000002) 15. Fixed the issue that some of the configured VLANs and port-channel information might disappear. (DRU20200526000002) 16. Fixed the issue that the source interface configuration would disappear after upgrade to beta firmware v1.14. (DI20200609000003) 17. Fixed the issue that the system would crash when configured LLDP feature. (DRU20200522000001) 18. Fixed the issue that when configured MVLAN (Multicast VLAN) feature, the switch would freeze for a while. (DEUR20200422000003) 19. Fixed the issue that user cannot use SNMP OID to display the VLAN

Mapping information correctly. (DRU20200519000005)

20. Fixed the issue that user cannot change the port mode to dot1q tunnel by using SNMP protocol. (DRU20200519000007, DRU20200512000001)

21. Fixed the issue that the IP interface would be cleared when user cleared VLAN Mapping configuration. (DRU20200519000004)

22. Fixed the issue that the Storm Control feature cannot be configured successfully by using SNMP protocol. (DRU20200519000003)

23. Fixed the issue that user cannot use SNMP OID to configure Spanning Tree Link Type feature. (DRU20200519000002)

24. Fixed the issue that the system would crash when worked with MAC-based Authentication feature. (DI20200508000006)

25. Fixed the issue that when user configured port channel feature and tried to display the configuration on CLI, the VLAN information was not complete or even disapper. (DRU20200526000002)

26. Fixed the issue that the DHCP Snooping with Option 82 parameter worked incorrectly. (DEUR20200506000003)

27. Fixed the issue that the IPv6 traffic counter cannot be queried by SNMP protocol. (DGC20200508000001)

28. Fixed the issue that the IGMP Snooping Querier needed to be enabled first so that swtich could display the information of querier's IP address. (DRU20200306000001)

29. Fixed the issue that when user fixed the port speed to 100M, switch still connected in 1000M. (DEUR20200309000002)

30. Fixed the issue that user cannot use Web GUI to configure port speed and when error happened, the configured port description would be cleared. (DEUR20200302000003)

31. Fixed the issue that when rebooting the switch, the OSPFv3 routing configuration would disapper. (DI20200401000002)

32. Fixed the issue that system will display "ERROR: Invalid IP address" information when configured loopback interface. (DI20200402000003)

33. Fixed the issue that when exporting the syslog to external syslog server, if switch's source IP address was not the same as the one of syslog server, switch would use 0.0.0.0 as the source IP address in the log message but not use the real one. (DUSA20200402000005)

34. Fixed the issue that when user stacked DGS-3130 and configured time-based PoE feature to disable PoE function in a specific time slot, the backup master swtich would still provide power to PD device. (DEUR20200406000002)

35. Fixed the issue that when tested MAC-based Access Control feature on DGS-3130 with specified number of MAC address. Switch could not learn the requested number. (DI20200403000005)

36. Fixed the issue that when configured swtich's log server to external one, the server would only receive IPv4 syslog message but not for IPv6. (DGC20200417000004)

37. Fixed the issue that switch's Device MAC and System MAC could not be acquired by quering associated SNMP OID. (DGC20200422000001)

38. Fixed the issue that when user configured SNMP community name with trusted host parameter together. The configuration would disappear after

rebooting the switch. (DRU20200423000003)

39. Fixed the issue that in stacking architecture, the Web GUI would freeze when user was configuring VLAN information. (DEUR20200121000001)

40. Fixed the issue that system would crash or freez when working with SNMP related features. (DI20200124000007, DI20200219000002, DI20200316000003, DI20200316000010)

41. Fixed the issue that if user keeped on logging in and logging out the switch when testing or using Web-based Authentication Access, the authentication page sometimes would not be found. (DI20200303000001)

42. Fixed the issue that the configured IP interface or static route configuration would loss after rebooting the device. (DRU20180921000002)

43. Fixed the issue that when switch worked with WAC authentication, the logout page may not be displayed. (DI20200303000001)

44. Fixed the issue that the CPU utilization would reach to 100% and the console would freaze as well. (DI20200316000003)

45. Fixed the issue that the design algorithm of OSPF SPF counter was not the same as other D-Link managed switches. (DI20200122000003)

46. Fixed the issue that swith sometime would display "Network login fail" message when working with WAC authentication. (DI20200121000005)

47. Fixed the issue that if user enabled WAC authentication on DGS-3130 and tried to open several authentication pages within a short interval, the login page may not display. (DI20200122000001)

48. Fixed the issue of several exception problems, switch would suddenly reboot without any notification. (DI20200124000006, DI20200207000001)

49. Fixed the issue that switch would display "Broken Pipe" information and user could not login the switch via console interface. (DI20200204000001)

50. Fixed the issue that user could not use SNMP to configure 802.1Q VLAN. (DUSA20200206000002)

51. Fixed the issue that when used Ping to test the connection status with IPv4 and IPv6 address, some packets would lost. (DGC20200107000002, DGC20200108000003)

52. Fixed the issue that when both IP Source Guard and ARP Inspection were enabled, some MAC addresses could not be learned correctly. (DEUR20200109000002)

53. Fixed the issue that the DHCP request packet's checksum was incorrect. (DI20200115000003)

54. Fixed the issue that the MAC address learning was not correct on port-channel interface. (DEUR20200109000002)

55. Fixed the issue that when user tried to configure VLAN, sometimes, the Web GUI would freeze. (DEUR20200121000001)

| V1.10.057 | 1. Fixed the issue that when user configured Voice VLAN on DGS-3130, the VoIP phones will get IP address from client VLAN but not from Voice VLAN. (DRU20190312000003) |
| | 2. Fixed the issue that the Trusted Host feature did not work correctly. |

(DGC20190508000001)

3. Fixed the issue that when user configured Voice VLAN and DHCP Snooping in physical stack architecture, the DHCP Snooping binding entries will be incorrect. (DRU20190528000001)

4. Fixed the issue that the ICMP packet cannot be dropped by ACL. (DRU20190603000001)

5. Fixed the issue that user cannot execute Ping command from multiple sessions, such as from console or telnet, at the same time. (DRU20190603000002)

6. Fixed the issue that when user enabled LLDP and trying to display neighbor's interface information, an incorrect interface ID will be displayed. (DRU20190614000002)

7. Fixed the issue that when user cleared switch's system log and running-config, user still can see port-channel link down information in system log but not an empty one. (DRU20190624000003)

8. Fixed the issue that switch will display unexpected log when user executed "clear counters" command. (DRU20190626000001)

9. Fixed the issue that when user enabled LBD (Loopback Detection) feature on DGS-3130 and then sending CDP packets in the network, switch's CPU utilization will rise. (DRU20190626000002)

10. Fixed the issue that switch cannot encrypt user's password with MD5 hash algorithm. (DRU20190617000004)

11. Fixed the issue that Q-in-Q cannot work with multicast VLAN. (DEUR20190206000003)

12. Fixed the issue that user cannot manage switch's file system via Web GUI when DGS-3130 working in the physical stacking architecture. (DEUR20190529000002)

13. Fixed the issue that when user used 3rd party transceiver connecting with DGS-3130-54S, some ports will not forward traffic. (DRU20181018000002)

14. Fixed the issue that DGS-3130 Series cannot work with DEM-410T transceiver. (DEUR20181109000004)

15. Fixed the issue that SNMPv3 with AES encryption algorithm cannot work. (DRU20190306000004)

16. Fixed the issue that when user configured forwarding IGMP traffic through Q-in-Q network, switch will remove the tag incorrectly. (DRU20190320000004)

17. Fixed the issue that the OSPF feature did not use wildcard mask but using netmask format. (DGC20190412000001)

18. Fixed the issue that the switch displayed incorrect statistics information of port interface. (DEUR20190502000001)

19. Fixed the issue that when sending TCP traffic from 10G to 1G interface, the transmission speed is much lower than expected. (DEUR20190528000003, DRU20190604000005)

20. Fixed the issue that when user tried to configure LACP via Web GUI on stacked switches, the configured port-channel interface will disappear when they tried to add other member switch's port into that port-channel group. (DEUR20190426000005, DEUR20190527000001)

21. Fixed the issue that the LDP packet cannot be forwarded by switch. (DRU20190527000001)

22. Modify the description of CLI console display when an interface's link status is down. (DRU20190226000003)

23. Fixed the issue that when user configured summer time, the setting will disappear after rebooting the switch. (DEUR20190424000002)

24. Fixed the issue that switch did not keep any system log in switch. (DEUR20190426000002)

25. Fixed the issue that when user disabled the learning from IMPB snooping, switch will keep on learning the entries. (DEUR20190416000002)

26. Fixed the issue that the system log discrimination feature did not work when user would like to filter specific log information. (DUSA20190507000003)

27. Fixed the issue that when user tried to display the status of loopback-detection, the system will display "*** Warning: Has deadlock taking order!!!! ***" information. (DGC20190513000001)

28. Fixed the issue that the loopback-detection function cannot work, and system might crash. (DGC20190513000002)

29. Fixed the issue that the GVRP function worked incorrectly. (DRU20190327000001)

30. Fixed the issue that switch had incorrect display for spanning tree information. Even though, there's no change for the spanning-tree mst configuration, console still displayed the content. (DRU20190329000002)

31. Fixed the issue that VLAN cannot be deleted via Web GUI. (DEUR20190402000005)

32. Fixed the issue that the untagged VLAN traffic was handled incorrectly and the configured configuration will change after reboot the switch. (DEUR20190408000001)

33. Fixed the issue that user cannot ping the target device in OSPF network even though the routing entries were all learned. (DGC20190412000002)

34. Fixed the issue that some configuration might loss after rebooting the physical stack. (DRU20190409000001)

35. Fixed the issue that user's password cannot send to RADIUS server (DGC20181107000005)

36. Fixed the issue that IP Helper feature cannot work on DGS-3130. (DRU20181211000003)

37. Fixed the issue that user cannot login switch's Web GUI with RADIUS' user account. (DRU20190123000002)

38. Fixed the issue that when user enabled Super VLAN and two PCs with different IP ranges, they still can ping each other successfully. (DRU20190226000001)

39. Fixed the issue that when user tried to create VLAN, DGS-3130 will always keep spanning tree log whether the status was enabled or not. (DRU20190226000002)

40. Fixed the issue that the DHCP discover packet which was received by DHCP Relay disabled port was not forwarded. (DRU20190301000004)

41. Fixed the issue that GVRP function did not work. (DRU20190228000002)

42. Fixed the issue that switch will drop DHCP discover packet if user disabled IGMP Snooping and then enabled it again. (DRU20190315000004)

43. Fixed the issue that the user authentication feature worked incorrectly, user can login the switch without password, even though AAA authentication was enabled already. (DRU20190211000003)

44. Fixed the issue that when DHCP Server Screening feature was enabled, switch did not keep correct DHCP Server. (DGC20190214000001)

45. Fixed the issue that when user enabled LBD (Loopback Detection) with VLAN mode, if the looped VLAN numbers were many, switch will miss detecting some looped VLANs. (DI20181113000005)

46. Fixed the issue that when switch received IGMPv3 leave report, DGS-3130 will remove the IGMP snooping entry immediately. (DI20181115000003)

47. Fixed the issue that when configured switch to filter unregistered multicast traffic, switch will filter some reserved multicast packets, such as PIMv6 hello, bootstrap, join or prune packets. (DI20181219000001)

48. Fixed the issue that when MAC authentication feature worked with multi-host or multi-auth authentication mode, switch will keep incorrect MAC entry in MAC address table. (DGC20190109000001)

49. Fixed the issue that there were some compatibility issues existed when working with Chrome, Opera and Microsoft Edge browser. (DEUR20190118000003)

50. Fixed the issue that when switch received MLDv2 Done message, DGS-3130 will remove the entry immediately. (DI20181213000003)

51. Fixed the issue that when authentication mode changed, the learned MAC address was not removed. (DI20181112000004)

52. Fixed the issue that when a client renews the IP address and sends a DHCP renew packet to DHCP server, the DHCP relay agent of switch will replay the packet; actually, the renew packet is a unicast packet to DHCP server and should not be replayed. (DI20181128000010)

53. Fixed the issue that DHCP Helper feature cannot work. (DRU20181211000003)

54. Fixed the issue that when issuing "debug copy tech-support" command, system will add incorrect line code in the end of each output debug information. (DI20180522000002, DI20181220000003)

55. Fixed the issue that the DHCP packet was also forwarded via Layer2 which behaved differently than other switch's behavior. (DI20181225000004)

56. Fixed the issue that switch did not forward the unicast DHCP packet when enabled relaying unicast DHCP packet. (DI20181225000003)

57. Fixed the issue that switch displayed the name of port channel group with port ID, such as eth0/3/1, but not using Port-channel1 naming. (DI20181227000003)

58. Fixed the issue that the inter-VLAN routing worked correctly but failed after rebooting the switch. (DI20181218000001)

59. Fixed the issue that when Link Aggregation (LAG) working with LBD function and a loop status occurred, the loop status display was incorrect

when just changed the link status of a member port. (DI20181115000001)

60. Fixed the issue that when copying files with brackets "()" in the file name, system will display 'shell error message sh:syntax error: unexpected "(" ' information. (DI20181212000002)

61. Fixed the issue that switch's Web GUI server sometimes did not response with client's connection request. (DI20181011000006)

62. Fixed the issue that when user tried to save the configuration file to a none existed file name, system will reply with "ERROR: File not found." error information. (DI20181220000002)

63. Fixed the issue that when user tried to copy the configuration file from TFTP server to running-config, system will display "% Invalid input detected at '^' marker." error message. (DI20181220000004)

64. Fixed the issue that the source IP interface's design of DGS-3130 was not the same as other D-Link managed switches. (DI20181003000007, DI20181226000001)

65. Fixed the issue that DGS-3130 cannot resolve AAAA record when querying the DNS server. (DI20181010000001)

66. Fixed the issue that the result of Cable Diagnostic was incorrect. (DI20181023000004)

67. Fixed the issue that user cannot use special character when configuring snmp-server parameters. (DUSA20181112000005, DGC20181107000002)

68. Fixed the issue that when switch running with ERPS configuration, if user rebooted the neighbor switch (RPL Neighbor), the connected port in RPL Owner switch will keep the up status for a while. (DI20181120000004)

69. Fixed the issue that if stacking member switch running with older firmware and also with not enough space in C:/ drive, the member switch will get into crash-and-reboot loop after PM switch finishes updating code to this member switch. (DI20181121000003)

70. Fixed the issue that when user logged in a switch via telnet, there will some unpredictable characters existed in user name's field. (DRU20181206000004)

71. Fixed the issue that when rebooting the switch, the priority configuration of Multiple Spanning Tree will be lost. (DI20181017000004)

72. Fixed the issue that the time range setting cannot work when user enabled it via CLI. (DI20181105000004)

73. Fixed the issue that the design of compound authentication of DGS-3130 is not the same as other D-Link managed switches. (DGC20181106000003)

74. Fixed the issue that sometimes the switch did not resend the authentication request to RADIUS server. (DGC20181107000007)

75. Fixed the issue that when user enabled LBD with VLAN mode function on switch; when a port with 4000 VLANs assigned encountered a loop status, all VLANs on the port became error disabled by LBD. User tried to recover the status by link-down and link-up action, VLAN 1~1024 were recovered when link down and VLAN 1025~2048 were recovered when link up; others remain in error disabled status. (DI20181113000009)

76. Fixed the issue that the stacking's master switch will reboot when user

tried to assign 4094 VLANs to member switch. (DI20181112000005)

77. Fixed the issue that when user changed the duplex mode of port interface, the port interface cannot link up. (DI20181018000003)

78. Fixed the issue that switch will accept DBCS (Double-Byte Character Set) as a user name which will cause authentication failure. (DI20181024000004)

79. Fixed the issue that when user disabled the management IP interface, the console will display "cat: read error: Invalid argument" incorrect error log. (DGC20181029000003)

80. Fixed the issue that user cannot configure 802.1Q-Tunnel VLAN mode via Web GUI. (DRU20181101000001)

81. Fixed the issue that switch will display "ERROR: TFTP transmission error" message when tried to copy files to flash. (DI20181102000005)

82. Fixed the issue that when user queried ifOctects MIB object for a non-existent stacking member switch, system will return incorrect value. (DI20181226000004)

83. Fixed the issue that when tried to change the management interface's configuration, the system will display "IP address and gateway do not reside on the same subnet" error information. (DRU20181204000003)

84. Fixed the issue that the switch will crash when tried to create untag VLANs. (DGC20181130000002)

85. Fixed the issue that the system will suddenly crash when configuring the switch. (DRU20181115000004)

86. Fixed the issue that switch will reboot when executed "show ipv6 mld snooping gr" command. (DI20181115000005)

87. Fixed the issue that the ERPS' protected VLAN can overlap with R-APS VLAN. (DI20181115000007)

88. Fixed the issue that switch cannot execute "show ip igmp snooping" command. (DI20181115000002)

89. Fixed the issue that the LBD's CTP frames were sent to all VLANs even user configured the LBD function with port-based mode. (DI20181112000003)

90. Fixed the issue that when user configured the traffic segmentation feature, switch will lose physical link on all ports after rebooting the switch. (DUSA20181112000004)

91. Fixed the issue that the ERPS Sub Ring status cannot change to "Idle" state. (DI20181120000003)

92. Fixed the issue that the sFlow packets cannot be sent to collector. (DGC20181108000002)

93. Fixed the issue that the packet from native VLAN still can reach to the destination port which was not belong to native VLAN. (DI20181106000002)

94. Fixed the issue that when user used DGS-712 transceiver on 10G SFP+ interface and used it to establish a LACP channel interface building a physical stacking, clients on each side of the stack cannot ping each other. (DRU20181010000005)

95. Fixed the issue that when RADIUS server was down, DGS-3130 still displayed the status as ON. (DGC20181030000003)

96. Fixed the issue that the statistics of IPv6 Ping was not correct. (DI20181102000004)

97. Fixed the issue that DHCP relay function was not work. (DI20181106000001)

98. Fixed the issue that the auto Voice VLAN feature cannot work correctly, user had to manually configure the Voice VLAN parameter. (IMA20181025000002)

99. Fixed the issue that when user fixed the speed or duplex mode of DGS-3130's port interface, the switch will fail to link with partner. (DI20181018000001)

100. Fixed the issue that the switch will fail to link with partner when working with auto negotiation mode. User had to fix the port speed to solve this issue. (DUSA20190307000001, DUSA20190307000002)

101. Fixed the issue that when user enabled Blat Dos Attack prevention with command "dos-prevention blat", switch will fail to block UDP packets. (DI20181024000002)

102. Fixed the issue that in the physical stack architecture, the files in the master switch cannot be copied to member switches. (DI20181023000003)

103. Fixed the issue that the system will crash when receiving PIMv2 hello packet. (DRU20181017000002)

104. Fixed the issue that if user configured MTU parameter, the IPv6 Ping will not work. (DI20181016000006)

105. Fixed the issue that user cannot save the master switch's RSA/DSA key to the slave one. (DI20181011000004)

106. Fixed the issue that in Primary Master (PM) switch election stage, the switch with higher stacking priority was not choosen as the PM role. (DRU20180809000002)

107. Fixed the issue that DGS-3130 used an expired certificate for SSL. (DI20181011000005)

108. Fixed the issue that the switch will delete all ARP entries at the same time even though some ARP entries' aging time were still not expired. (DI20181005000004)

109. Fixed the issue that when user configured an illegal subnet mask, such as using only 1 leading 1-bit with CIDR format, system still accepted the configuration. (DI20181004000002)

110. Fixed the issue that switch will send extra ping packet to destination which will cause an incorrect statistics number. (DI20181003000003)

111. Fixed the issue that the disk size of USB cannot be displayed by both CLI and Web GUI. (DRU20180924000003)

112. Fixed the issue that when user configured the SMTP settings via Web GUI, the switch will fail to send any email to the receiver. (DGC20180919000003)

113. Fixed the issue that if user successfully configured a static route from the Web GUI, this action will create a CLI command but will not work in CLI console. (DGC20180919000003)

114. Fixed the issue that the created VLAN cannot be deleted by Web GUI. (DGC20180919000003)

115. Fixed the issue that the system will return an error message "ERROR: Not a valid firmware file", when tried to backup the firmware file via the Web GUI. (DGC20180919000003)

116. Fixed the issue that when user issued a trace route command via the Web GUI, and then clicked the "Back" button, there was no response for this action. (DGC20180919000003)

117. Fixed the issue that the Port Security did not work correctly. (DGC20180919000003)

118. Fixed the issue that if user created IP interface without configuring IP address, the interface with no IP address cannot be displayed on the console. (DRU20180921000002, DRU20181002000003)

119. Fixed the issue that user cannot telnet the switch and the console will also be frozen at the same time when DGS-3130 working on Stacking architecture. (DEUR20190610000001)

120. Fixed the issue that user cannot enable or disable the PoE trap on DGS-3130. (DRU20190618000002)

121. Fixed the issue that when user enabled LLDP-MED on DGS-3130, user's IP phone cannot get Voice VLAN information from DGS-3130. (DRU20190606000002)

122. Fixed the issue that the jumbo frame configuration will not work when configured on channel-group interface. (DEUR20190708000004)

123. Fixed the issue that when switch received IGMP join packet, switch's uptime timer will be reset. (DEUR20190710000001)

124. Fixed the issue that when user executed the command "no interface vlan 1" to remove interface vlan 1 and then queried OID 1.3.6.1.2.1.2.2.1 with snmpwalk tool, the switch will not response after quering the OID for a while. (DGC20190711000001)

125. Fixed the issue that user cannot see Slave switch's environment information from Web GUI, only Master switch can be seen. (DEUR20190712000001)

126. Fixed the issue that when user tried to change the stacking priority through the Web GUI, the change will not take effect. (DEUR20190708000009)

127. Fixed the issue that DGS-3130 will create duplicated IPv6 snooping entries when enabling DHCPv6 Snooping. (DEUR20190705000005)

128. Fixed the issue that when user copied new configuration file from TFTP server to replace the old one in the switch, the new IP interface in the configuration file will not be applied. (DRU20190715000003)

129. Fixed the issue that when user configured trusted host feature and a client in invalid IP range, the client still can access the switch. (DGC20190508000001)

130. Fixed the issue that when user issued "clear running-config" command on Master switch, the system will enter exception mode. (DRU20190624000003)

131. Fixed the issue that when queried Web GUI's *Port Configuration > Port Status* information, the information in the table may incorrect. (DEUR20190722000003)

132. Fixed the issue that when both IGMP Snooping and Port-based Q-in-Q

were enabled on DGS-3130, customers had problem in receiving multicast packets. (DRU20190726000002)

133. Fixed the issue that when enabled the IMPB function on DGS-3130, the valid VoIP device will be treated as an invalid client. (DRU20190801000003)

134. Fixed the issue that when user configured "logging source-interface" command, the user configured command did not add into the running configuration. (DRU20190809000002)

135. Fixed the issue that the "monitor session destination interface" configuration will be dropped when user configured port mirror feature. (DRU20190812000001)

136. Fixed the issue that DGS-3130 will keep incorrect uptime timer for IGMP Snooping Group. (DEUR20190816000006)

137. Fixed the issue that when user assigned an IP interface as the TFTP's source interface, DGS-3130 did not use the assigned IP interface as the source IP but use the Management IP Interface as the source. (DRU20190812000002)

138. Fixed the issue that sometimes the switch will not recive the IGMP Join packet sending from clients. (DEUR20190917000009)

139. Fixed the issue that user cannot configure SNMPv3 with AES encryption algorithm. (DRU20190306000004)

140. Fixed the issue that when user connected the switch by Web GUI or console port, the connection may not stable. (DEUR20190719000002)

141. Fixed the issue that when DGS-3130 sent the command log to TACACS+ server, the log did not contain the privilege level; also some attributes will be duplicated. (DRU20190808000005)

142. Fixed the issue that when user configured selective Q-in-Q feature, once user changed the VLAN mapping rule, the feature will not work. (DRU20190821000003)

143. Fixed the issue that when DGS-3130 working on stacking architecture and user copied the running-config to startup config, the boot configuration did not synchrionize to slave switches. (DRU20190910000005)

144. Fixed the issue that there's no timestamp in DGS-3130's syslog message. (DEUR20190918000002)

145. Fixed the issue that when enabling IMPB on DGS-3130, the switch did not block the IPv6 access whose IPv6 prefix was not in the white list. (DEUR20190905000004)

146. Fixed the issue that when user configured the command "configure replace tftp", the system will crash. (DRU20191001000005)

147. Fixed the issue that the telnet session will be terminated after configuring snmp-server name configuration. (DRU20191007000002)

148. Fixed the issue that there's a "description" parameter under "interface vlan" command but actually user cannot configure it. (DRU20191008000001)

149. Fixed the issue that the command logging feature will not log the command action which was configured under "interface ethernet" parameter. (DRU20191011000001)

150. Fixed the issue that when DGS-3130 enabled PBR feature, sometimes the system will hangup. (DGC20191022000001)

151. Fixed the issue that if user used thired party's transceiver, DGS-3130 cannot identify it. (DEUR20191016000006)

152. Fixed the issue that when enabled MAC-Based Access Control, the system will not count down the "aging time" number. (DRU20191008000004)

153. Fixed the issue that the QoS feature did not work correctly. (DEUR20191010000003, DEUR20191007000006)

154. Fixed the issue that the aging time of MAC-Based Access Control cannot configure to 24 hours (86400 seconds). (DRU20191009000001)

155. Fixed the issue that switch's FDB table will display incorrect MAC and VLAN binding information when enabled MAC-Based Access Control feature. (DRU20191015000007)

156. Fixed the issue that the Port Mirror feature cannot support configuring four ingress mirror sessions. (DRU20191016000001)

157. Fixed the issue that when DGS-3130's PBR feature worked with two ECMP enabled default routes, the route may not correct. (DGC20191023000003)

158. Fixed the issue that when IPTV customer changed the TV channel, it took about 20 seconds to complete it. (DEUR20191111000007)

159. Fixed the issue that when user enabled IP-MAC-Port Binding feature and keep on running for a period of time, system may suddenly crash. (DEUR20191111000003)

160. Fixed the issue that there's no MIB support for configuring "Port Speed", "Auto Speed Downgrade" and "Set Advertised Port Speed" features. (DUSA20190924000002)

161. Fixed the issue that when user configured Port Security feature on DGS-3130 and specified a MAC address as a Permanent status, the specified MAC address will be removed after unplug the connected port. (DEUR20191107000004)

162. Fixed the issue that when configuring the Expert ACL with "None" option in Protocol Type parameter via switch's Web GUI, the system will add protocal number "255" automatically. (DGC20191115000002)

163. Fixed the issue that in stacking architecture, the Web GUI cannot display the information in "STP Port Settings" page but no such issue with standalone switch. (DRU20191113000001)

164. Fixed the issues of incorrect neighbor solicitation behavior and also for the incorrect display of IPv6 ND Snooping binding entries' lease time. (DEUR20191120000009)

165. Fixed the issue that the "Syslog hostname" information in DGS-3130's syslog displayed an incorrect string "Wrong-family-addr" but not display an IP address. (DRU20191121000001)

166. Fixed the issue that sometimes DHCP clients cannot get IP addresses assigned from DHCP server which were dropped by DGS-3130. (DRU20190312000004)

V1.01.B027	Fixed the issue that when loop occurred, the affected port will remain on error disabled status and cannot back to normal. (DGC20180810000002)
V1.01.026	First Release

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues	Workaround/Status
V1.16.002	1. When configured SNTP feature, it will fail to do SNTPv6 time refresh in the first attempt after switching from SNTPv4. However, the 2nd attempt will be success.	Trying to shorten the refresh interval by using following command: *Switch(config)#sntp interval*
	2. There's hardware limitation of DDM on DEM-410T	No influence for data transmission, only DDM cannot work.
V1.10.057	1. The Power Saving feature cannot work on stacking architecture.	There's no problem to work on standalone switch.
	2. The Cable Diagnostic feature cannot work at port 9 to 24 of DGS-3130-30TS	It's a limitation of current chip.
	3. The Cable Diagnostic feature cannot work at port 9 to port 24 and port 33 to port 48 of DGS-3130-54TS	
	4. There's hardware limitation of DDM on DEM-410T	No influence for data transmission, only DDM cannot work.
	5. In stacking architecture, if user configures "l2protocol-tunnel global drop-threshold" command, when slave switch rebooted, this configuration cannot work on slave switch.	There're two workarounds for this issue: 1. Reboot the PM switch 2. Disable and then enable L2PT again. - CLI command example: *Switch#configure terminal* *Switch(config)#interface ethernet 2/0/11* *Switch(config-if)#no l2protocol-tunnel stp* *Switch(config-if)#l2protocol-tunnel stp*
	6. The ERPS sub-ring will enter incorrect ring state to display Protection status when link failover, but it still blocks the loop.	The workaround steps 1. To force switch PORT0 for the ring with wrong state. 2. Clear force switch 3. CLI command example: *Switch#configure terminal* *Switch(config)#ethernet ring g8032 ring2* *Switch(config-erps-ring)#instance 2* *Switch(config-erps-ring-instance)# erps force switch ring_port port0* *Switch(config-erps-ring-instance)# clear*

V1.01.026	1. The first DAD NS packet is missing while an IPv6 node directly connects to DGS-3130 and ND snooping does not learn it into a binding table.	Waiting for BRCM's SDK fix patch.
	2. Prompt information "This is TACACS" is set on the TACACS+ server. While doing telnet to DGS-3130 via TACACS+ server, CLI will not show "This is TACACS" information.	Fix in the next release.
	3. "Backspace" cannot be used as DELETE function	Fix in the next release.
	4. When rebooting DGS-3130, "unsaved changes" information shows even there is no changes.	Fix in the next release.
	5. Do not support "Ctrl + C" to interrupt continuous message displays.	Fix in the next release.
	6. After breaking stacking connections in a two switches system, the LACP group cannot be established between these two switches because BM inherits PM's system MAC address and MACs are conflict.	Reboot the original BM switch first before establishing the LACP group.
	7. In Stacking Lite, Chain topology is not recommended.	Using Ring topology.

* D-Link tracking number is enclosed in ()

Related Documentation:

- DGS-3130_Series_A1_CLI Reference Guide_v1.20
- DGS-3130_Series_A1_HW Installation Guide_v1.00
- DGS-3130_Series_A1_Web UI Reference Guide_v1.20