Firmware Version: 2.02.030
MIB Version: DGS-1250_MIB_Files_20201204.zip
D-View Module Version: NA
Published: Jan. 29, 2021

Note: If the device is with less and equal to 1.00.040 version of firmware, please follow up this procedure to upgrade firmware to v2.01 successfully.

1. **Upgrade a temporary firmware v2.00.013, making sure the device is with firmware v2.00.013.**
2. **Upgrade firmware v2.01 to device**

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 via Telnet 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: v1.00.039	13-Jun.-19	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1
Runtime: v1.00.040	7-Oct.-19	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1
Runtime: v2.1.006/2.00.013	17-Dec.-19	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1
Runtime: v2.2.030	29-Jan-21	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1

Upgrade Instructions:

D-Link Smart 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 (via Telnet)

1. Make sure the network connection between the switch and PC is active.
2. Use software that supports telnet, for example, HyperTerminal or Telnet command in Microsoft Windows, to connect to the switch. If you are using Telnet command, type the command followed by the switch IP address, eg. *telnet 10.90.90.90*.
3. The logon prompt will appear.

The switch will prompt the user to enter his/her username and password. It should be noted that upon the initial connection, both the default user name and password are **admin**.

To upgrade the switch firmware, execute the following commands:

Command	Function
copy tftp://location/filename flash: {Image1|Image2}	Download firmware file from the TFTP server to the switch.
Boot image {Image1|Image2}	Change the boot up image file.
Show boot	Display the information of current boot image and configuration.

reboot	Reboot the switch

Example:

DGS-1250-28X:
Command: copy tftp: //10.90.90.99/DGS1250/DGS-1250_Run_1_00_039.had flash: Image1

Address of remote host [10.90.90.99]?
Source filename [DGS1250/DGS-1250_Run_1_00_039.had]?
Accessing tftp:// 10.90.90.99/DGS1250/DGS-1250_Run_1_00_039.had...
Transmission start...
Transmission finished, file length 8709008 bytes.
Please wait, programming flash..... 100 %
Please wait, programming flash for language files .....Done.

Switch#
Switch#configure terminal
Switch(config)#boot image Image1
Switch(config)#end
Switch#sh boot

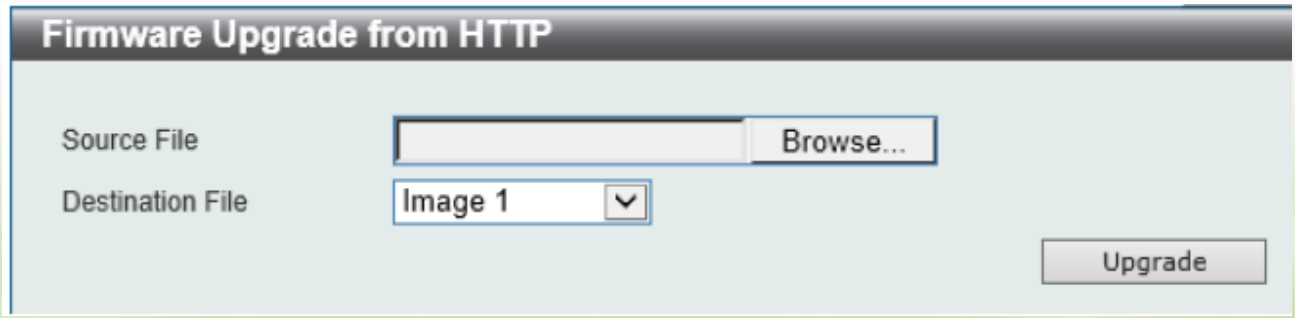
Unit 1
Boot image: /c:/Image1
Boot config: /c:/Config1

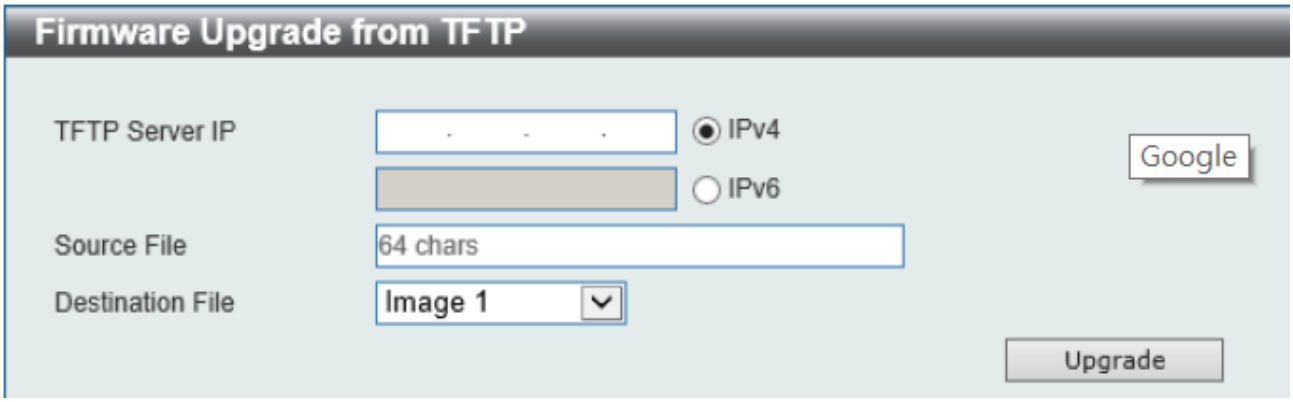
Switch#reboot

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

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 password when prompted. The password is **admin** by default.
4. Two methods can be selected to update switch's firmware or configuration file. A. Go to ***Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP*** from the banner. B. Go to ***Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP*** from the banner.

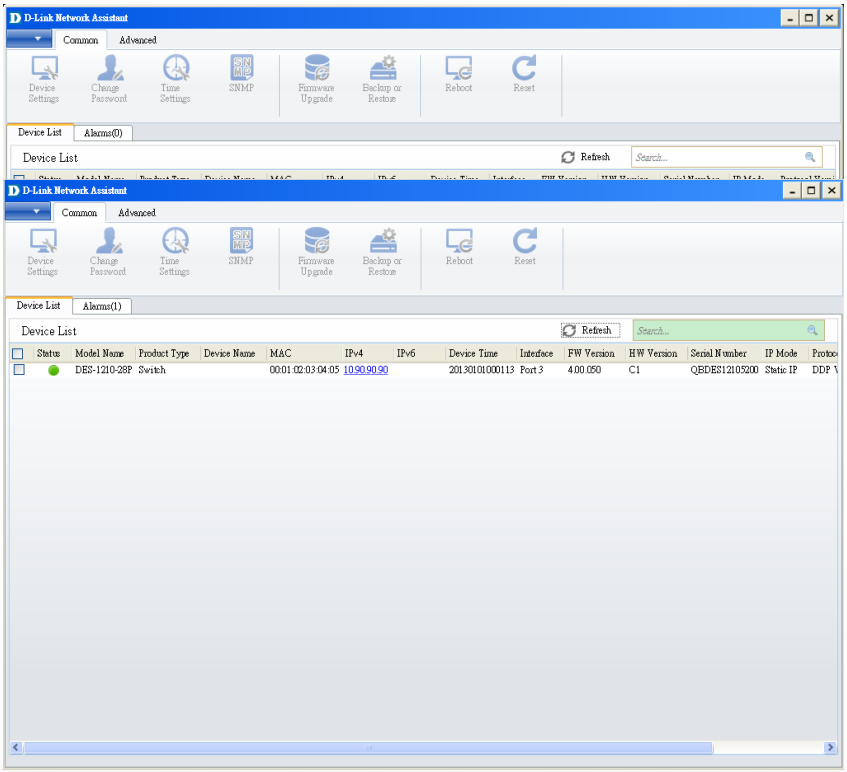




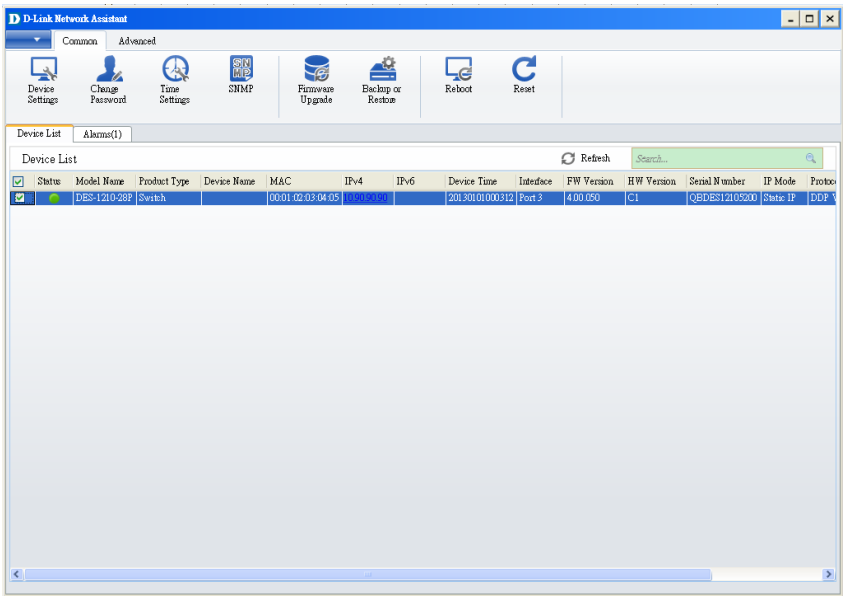
Upgrade using D-Link Network Assistant

1. Connect a workstation installed with java SE runtime environment to any switch port of the device

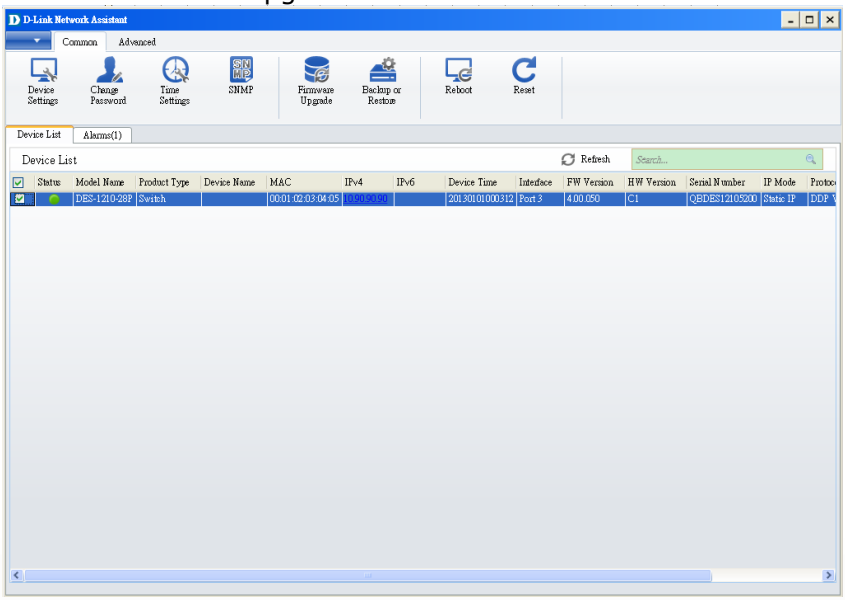
1. Execute D-Link Network Assistant



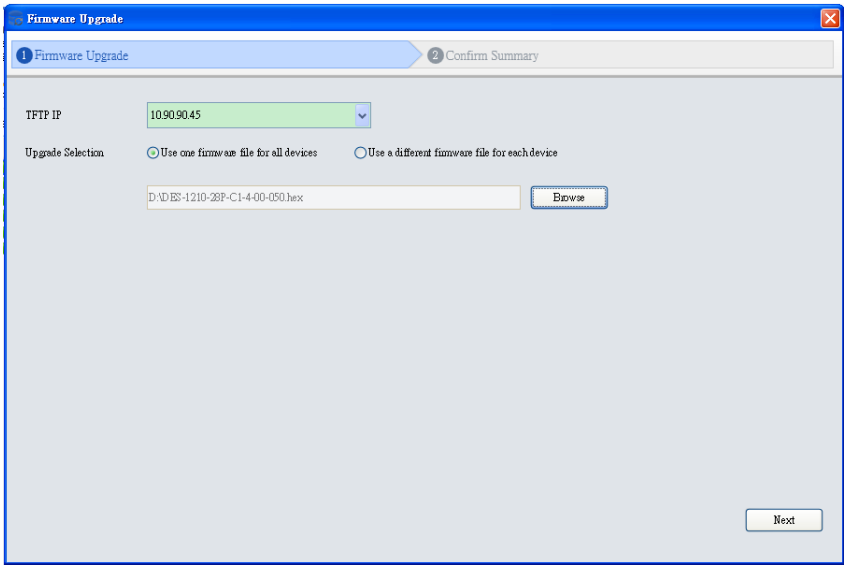
4. Single click the icon of the column to choose the target switch



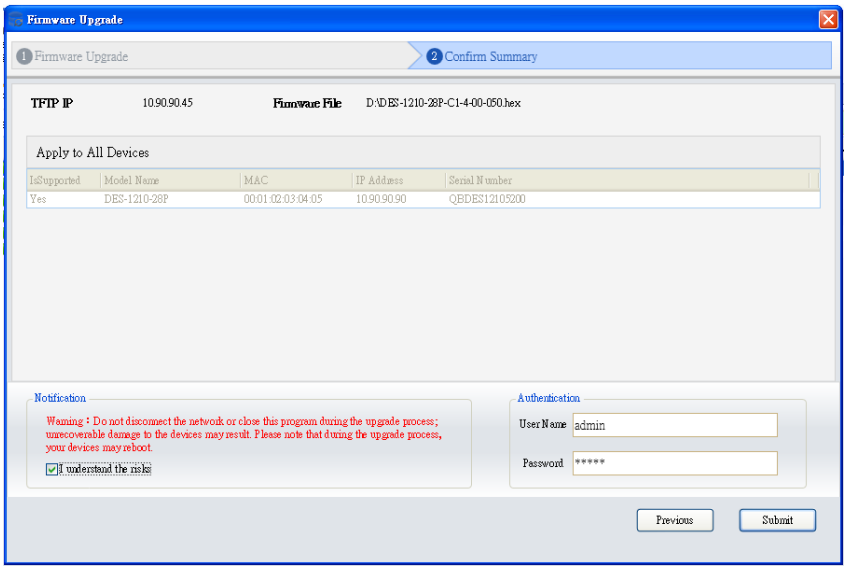
5. Click Firmware Upgrade button



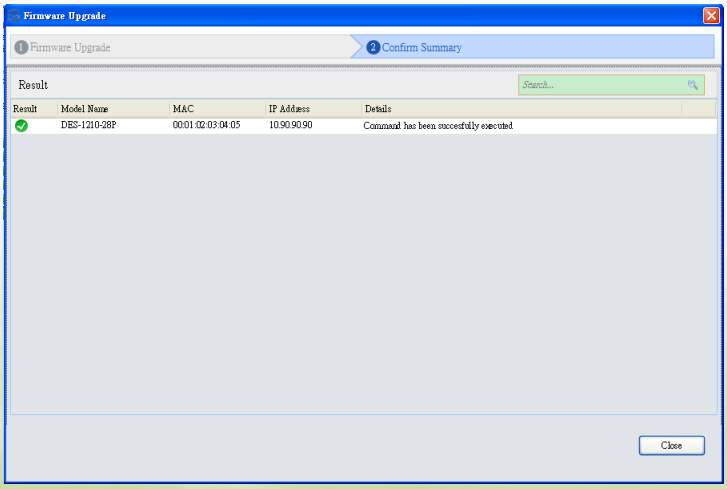
6. Select PC IP address is used to connect the target switch, then click Browse button and select the firmware file (Model name_HW ver._FW ver. .hex) on your local hard drive.



7. Click the checkbox and click "Submit" button to start firmware upgrade.



8. Once the message changed to success, click "Close" button to complete and exit the firmware upgrade



New Features:

Firmware Version	New Features
V1.00.039	First Release
V1.00.040	N/A
V2.01.006/2.00.013	1. Full feature command line 2. SNMP trap - New MAC notification with VLAN ID 3. PD alive 4. 802.1x host-based access control 5. Supports Do command Note: The new firmware V2.0x.xxx is not backward compatible with V1.00.xxx.
V2.02.030	1. AAA Support for RADIUS/TACACS+ 2. MAC Authentication 3. Password encryption 4. Command logging 5. DDM support for optics 6. Enhanced SSH key exchange to SHA2 256bytes. [DI20201130000004]

Changes of MIB Module:

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

Firmware Version	MIB File	New Features
V1.00.039	DGS-1250_MIB_Files_20190320.zip	First Release
V1.00.040	No change	
V2.01.006	DGS-1250_MIB_Files_20190731.zip	
V2.02.030	DGS-1250_MIB_Files_20201204.zip	

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
V1.00.039	N/A
V1.00.040	N/A
V2.01.006	Support Full CLI
V2.02.030	Add the following CLI support: 1. AAA Support for RADIUS/TACACS+ 2. MAC Authentication 3. Password encryption 4. Command logging 5. DDM support for optics 6. Support SSH public key file upload by CLI 7. Show privilege command changed from "Current privilege level is 15" to "Current level is Privilege level"

Problem Fixed:

Firmware Version	Problems Fixed
V1.00.039	1. [DBG19040640] The hop count value does not increase 1 when DHCP discover packets relay to DHCP server. (Will Fix in R2) 2. [DBG19040649] The 802.1X RADIUS Statistic are up when the status of server 1 is entering deadtime. (Will Fix in R2) 3. [DBG19050009] The behavior of 802.1X unauthenticated port and authenticated port are abnormal. (Will Fix in R2) 4. [DBG19040521] IGMP Snooping web button error. (Will Fix in R2) 5. [DBG19040443] Deleting specific VLANs will show success but it does not exist in VLAN entries. (Will Fix in R2) 6. [DBG19040181, DBG19040204] Reserved Multicast addresses packets

	will be captured at the receiver more than sender. (Will Fix in R2) 7. [DBG19040355]DUT will not reply ping packet with jumbo frame. (Will Fix in R2) 8. [DBG19040523] There is no warning message for un-existed time profile on Power Saving page. (Will Fix in R2) 9. [DBG19040533] DUT cannot recognize some IPCams(D-link/Hikvision/Dahua) (Will Fix in R2) 10. [DBG19040520] DUT will mirror few packets under full packet rate. (SW RD will improve on R2)
V1.00.040	1. Fixed the fan LED error issue
V2.01.006	1. The Packets will not be mirrored when the packets meet the ACL deny rule. 2. [DBG19040640] The hop count value does not increase 1 when DHCP discover packets relay to DHCP server. 3. [DBG19040649] The 802.1X RADIUS Statistic are up when the status of server 1 is entering deadtime. 4. [DBG19050009] The behavior of 802.1X unauthenticated port and authenticated port are abnormal. 5. [DBG19040521] IGMP Snooping web button error. 6. [DBG19040181, DBG19040204] Reserved Multicast addresses packets will be captured at the receiver more than sender. 7. [DBG19040355] DUT will not reply ping packet with jumbo frame. 8. [DBG19040533] DUT cannot recognize some IPCams (D-Link/Hikvision/Dehua) 9. [DBG19040520] DUT will mirror few packets under full packet rate. 10. DBG19110242: [DHCP Relay plus DHCP Snooping] Error log occurred after Client get IP 11. DBG19110340: [CLI/IMPB] Configure "ip verify source vlan dhcp-snooping" failed. 12. DBG19110347: [802.1X device configure multi-auth mode] When configure multi-auth mode, CLI doesn't show error message to let user know unable to initialize as multi-auth mode, but WEB GUI works normally. 13. DBG19110348: [802.1X] When 802.1X is disabled, DUT should not be allowed to initialize by port. 14. DBG19110431: [802.1X] Re-authenticate by port does not work normally on CLI.

	15. DBG19040727: Unable to change time by NTP/SNTP server 16. DBG19110878: [CLI/LBD] Sometimes device will reboot with crash exception log after enabling LBD. This issue is random and cannot be duplicated every time.
V2.02.030	1. Low level of security for SSH sessions [DI20201130000004-Australia]. DGS-1250 current supported SSH key exchange is diffie-hellman-group1-sha1 (768 bits). This new firmware supports newer algorithm diffie-hellman-group-exchange-sha256. 2. Tagged traffic increment errors no matter the true size of the packet [DUSA20201112000003-USA]. Fixed the problem that the tagged packets cannot be calculated in error packet type. 3. DGS-1250-xx - EDIMAX WIFI Solution issue [DEUR20201124000004-Central Europe]. The CAPWAP packet, in which the destination UDP port is 5246/5247, will be dropped by DGS-1250 series 52 port models, causing the Wireless AP cannot be discovered by AP controller. This new firmware adds workaround to forward CAPWAP packet. 4. Russia language problem on Web GUI [DRU20200421000005]. Corrected the Russian language drop-down menu of local Web GUI, which originally displayed "Языковой", corrected to "Язык". 5. [DEUR20200305000008-Eastern Europe] Port rate limiting: The input/output burst size changed from 0-128000kbytes to 0-64kbytes 6. Web add checkbox "Default" to "Log buffer entries" in "DHCP Server Screening Global Settings" page for making settings change to Default. 7. The year range changed from "2000-2099" to "2000-2069". Copyright year changed from 2020 to 2021 8. Device Information page for removing FLASH which will be not support by Chrome. 9. Web to Disabled "textbox" while "UDF" selected as "None" in "DHCPv6 Relay Global Settings" page 10. Modify Introduction string in "DHCP Auto Configuration" page 11. Remove "Distance/Metric" column on IPv4 route & IPv6 route web page and CLI show IPv4 route & show IPv6 route command.

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware	Issues	Worka

Version		round
V1.00.039	N/A	
V1.00.004	N/A	
V2.01.006	1. [DBG19040443] Deleting specific VLANs will show success but it does not exist in VLAN entries. 2. [DBG19040523] There is no warning message for un-existed time profile on Power Saving page. ***Chip Limitation:*** 3. In the current design, NDP packets(ICMPv6 type 133~137) cannot be deny the HW forward packets by user ACL. It is chip limitation for DGS-1250. 4. The destination port numbers 5246 and 5247 are used for CAPWAP data and control packets in the RTL9310 chip. If the switch checks that the header is invalid, the default action of both packets will be dropped. The 2 packets (UDP Dst port 5246 5247) on 9310(52X/52XMP) will be drop. The 2 packets (UDP Dst port 5246 5247) on 9300(28X/28XMP) will be forward. 5. Dynamic ARP entries cannot be kept when the related L2 entry age-out 6. If aging time of "ARP" is greater than aging time of "MAC address", when MAC address is aged out, the corresponding ARP entries will be aged out, too.	
V2.02.030	***Chip Limitation:*** 1. In the current design, NDP packets(ICMPv6 type 133~137) cannot be deny the HW forward packets by user ACL. It is chip limitation for DGS-1250. 2. Dynamic ARP entries cannot be kept when the related L2 entry age-out 3. The input rate limit for TCP traffic on DGS-1250-28X and DGS-1250-28XMP would not be accuracy when the input rate limit is setting below 100Mbps. 4. The ingress rate limit on DGS-1250 would have higher rate limit then the setting at the beginning of the traffic, but it will be down to the rate limit setting after 1~2 seconds.	

Related Documentation:

- DGS-1250 Series A1 Web Manual, CLI Manual, Hardware Manual V2.0
- DGS-1250 Series A1 Getting Started Guide