



Firmware Version: 2.10.004
MIB Version: DGS-1250_R2.10
 _MIB_Files_20240417.zip
Published: Apr. 25, 2025

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:

Upgrade Instructions:	3
Upgrade using CLI (via Telnet).....	3
Upgrade using Web-UI.....	4
New Features:.....	5
Changes of MIB Module:	6
Changes of Command Line Interface:	7
Problem Fixed:	10
Known Issues:	16
Related Documentation:	18

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
Runtime: v2.3.004	03-Jun-21	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1
Runtime: v2.04.B006	31-March-23	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1
Runtime: v2.04.003	31-March-23	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1/A2
Runtime: v2.04.P004	15-May-23	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1/A2
Runtime: v2.10.004	17-Apr-24	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1/A2
Runtime: v2.10.005	27-May-24	DGS-1250-28X DGS-1250-28XMP DGS-1250-52X DGS-1250-52XMP	A1/A2

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
```

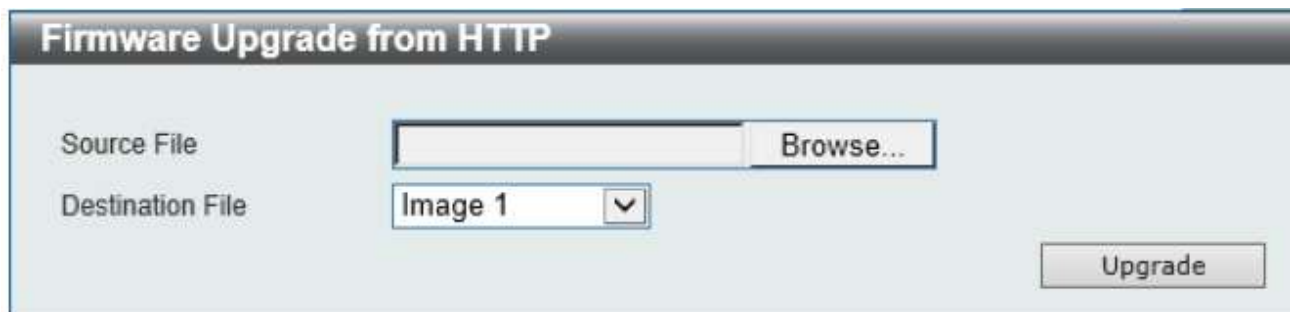
```
Unit 1
Boot image: /c:/Image1
Boot config: /c:/Config1
```

```
Switch#reboot
```

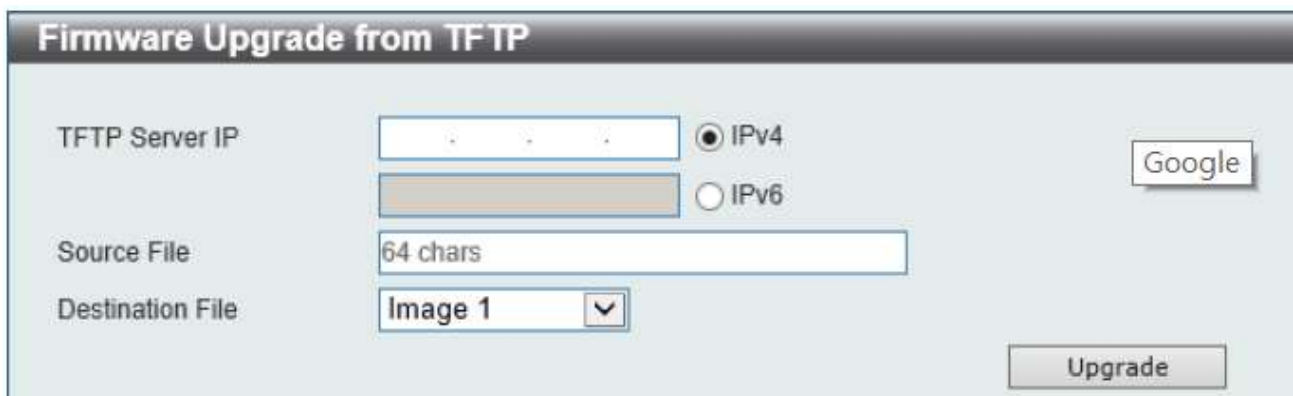
Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...

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.



The screenshot shows the 'Firmware Upgrade from HTTP' web interface. It has a title bar at the top. Below it, there are two main sections: 'Source File' and 'Destination File'. The 'Source File' section has a text input field and a 'Browse...' button. The 'Destination File' section has a dropdown menu currently showing 'Image 1'. At the bottom right of the interface is an 'Upgrade' button.



The screenshot shows the 'Firmware Upgrade from TFTP' web interface. It has a title bar at the top. Below it, there are several fields: 'TFTP Server IP' with a text input field and a radio button for 'IPv4' (which is selected) and another radio button for 'IPv6'. There is a 'Google' button next to the IP fields. Below these are 'Source File' and 'Destination File' sections. The 'Source File' section has a text input field with '64 chars' inside. The 'Destination File' section has a dropdown menu currently showing 'Image 1'. At the bottom right of the interface is an 'Upgrade' button.

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]
V2.03.004	N/A
V2.04.B006	N/A
V2.04.003	N/A
V2.04.P004	Add new feature with CLI + SNMP MIB 1. Support "show interface gbic" 2. Support Non-WAC Function
V2.10.004	1. Support show interface gbic 2. Support Reboot schedule 3. Support Support Non-WAC Function w/ CLI + SNMP MIB(SNR-20230105-001) 4. Support SNR-20211125-002(SSH Weak Algorithms) 5. Support SNR-20220119-001(New ciphers for SSH) 6. Support JQuery version 3.5.0 or later 7. Openssl upgrade to at least "1.1.1l" or latest version

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	
V2.03.004	N/A	
V2.04.B006	N/A	
V2.04.003	N/A	
V2.04.P004	DGS-1250_R2.04P_MIB_Files_20230331.zip	
V2.10.004	DGS-1250_R2.10_MIB_Files_20240417.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"
V2.03.004	N/A
V2.03.B006	N/A
V2.04.003	N/A
V2.04.P004	Add the following CLI support: 1. RADIUS CoA&DM (RFC5176) for Non-WAC 2. NAS-Identifier (RADIUS Attribute 32) for Non-WAC 3. NAS-IP-Address (RADIUS Attribute 4) for Non-WAC 4. Tunnel-Private-Group-ID (RADIUS Attribute 81) for Non-WAC 5. show interface gbic
V2.10.004	1. Non-WAC RADIUS CoA&DM (RFC5176) Added following command:

```
aaa server radius dynamic-author
no aaa server radius dynamic-author
client { IP-ADDRESS | HOSTNAME } server-key [ 0 | 7 ] STRING
no client { HOSTNAME | IP-ADDRESS }
port PORT-NUMBER
no port
radius-server attribute 55 include-in-acct-req
no radius-server attribute 55 include-in-acct-req
```

NAS-Identifier (RADIUS Attribute 32)

Added following command:

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the radius-server attribute 32 include-in-access-req global configuration command. To use system name sending RADIUS attribute 32 (backwards compatible), use the no form of this command.

```
radius-server attribute 32 include-in-access-req STRING
no radius-server attribute 32 include-in-access-req
```

NAS-IP-Address (RADIUS Attribute 4)

Added following command:

```
radius-server attribute 4 IP-ADDRESS
no radius-server attribute 4 IP-ADDRESS
```

Tunnel-Private-Group-ID (RADIUS Attribute 81)

No UI

RADIUS support Source Interface

Added following command:

```
ip radius source-interface INTERFACE-ID
no ip radius source-interface
ip tacacs source-interface INTERFACE-ID
no ip tacacs source-interface
ipv6 radius source-interface INTERFACE-ID
no ipv6 radius source-interface
ipv6 tacacs source-interface INTERFACE-ID
no ipv6 tacacs source-interface
```

Support Network Accounting

Added following command:

```
aaa accounting network default {start-stop METHOD1 [METHOD2...] | none}
```

no aaa accounting network default

Modified following command:

```
radius-server host {IP-ADDRESS | IPV6-ADDRESS } [auth-port PORT]
[acct-port PORT] [timeout SECONDS ] [retransmit COUNT ] key [0 | 7] KEY-STRING
```

2. show interface gbic

```
show interfaces [INTERFACE-ID [, | -]] gbic
```

3. reboot schedule

```
reboot schedule {in MINUTES | at HH:MM [DDMTHYYYYY]}
[save_before_reboot]
```

no reboot schedule

```
show reboot schedule
```

4. SSH

```
ip ssh server algorithm encryption { [aes128-cbc] [aes192-cbc]
[aes256-cbc] [3des-cbc] [blowfish-cbc] [twofish128-cbc] [twofish192-cbc]
[twofish256-cbc] [arcfour] [cast128-cbc] [aes128-ctr] [aes192-ctr]
[aes256-ctr] [aes128-gcm@openssh.com][aes256-
```

```

gcm@openssh.com][chacha20-poly1305@openssh.com]]
no ip ssh server algorithm encryption { aes128-cbc | aes192-cbc |
aes256-cbc | 3des-cbc | blowfish-cbc | twofish128-cbc | twofish192-cbc
| twofish256-cbc | arcfour | cast128-cbc | aes128-ctr | aes192-ctr |
aes256-ctr | aes128-gcm@openssh.com | aes256-gcm@openssh.com |
chacha20-poly1305@openssh.com}
ip ssh server algorithm key-exchange {[{diffie-hellman-group1-sha1}]
[{diffie-hellman-group14-sha1}][{diffie-hellman-group14-sha256}]
[{diffie-hellman-group16-sha512}] [{diffie-hellman-group18-
sha512}][{diffie-hellman-group-exchange-sha1}] [{diffie-hellman-
group-exchange-sha256}] [{ecdh-sha2-nistp256}][{ecdh-sha2-
nistp384}] [{ecdh-sha2-nistp521}] [{curve25519-sha256}]]}
no ip ssh server algorithm key-exchange {diffie-hellman-group1-sha1 |
diffie-hellman-group14-sha1 | diffie-hellman-group14-sha256 | diffie-
hellman-group16-sha512 | diffie-hellman-group18-sha512 | diffie-
hellman-group-exchange-sha1 | diffie-hellman-group-exchange-sha256
| ecdh-sha2-nistp256 | ecdh-sha2-nistp384 | ecdh-sha2-nistp521 |
curve25519-sha256}
ip ssh server algorithm mac { [hmac-sha1] [hmac-sha1-96] [hmac-
md5] [hmac-md5-96] [hmac-sha2-256]}
no ip ssh server algorithm mac {hmac-sha1| hmac-sha1-96 | hmac-
md5 | hmac-md5-96 | hmac-sha2-256}
ip ssh server algorithm hostkey {ssh-dss| ssh-rsa}
no ip ssh server algorithm hostkey {ssh-dss| ssh-rsa}
5. SSL
no ssl-service-policy <string 1-32> [ { version [ { tls1.0 } ]
[ { tls1.1 } ] [ { tls1.2 } ] | ciphersuite [ { dhe-dss-3des-ede-cbc-
sha } ] [ { rsa-3des-ede-cbc-sha } ] [ { rsa-rc4-128-sha } ] [ { rsa-rc4-
128-md5 } ] [ { rsa-export-rc4-40-md5 } ] [ { rsa-aes-128-cbc-sha } ]
[ { rsa-aes-256-cbc-sha } ] [ { rsa-aes-128-cbc-sha256 } ] [ { rsa-aes-
256-cbc-sha256 } ] [ { dhe-dss-aes-256-cbc-sha } ] [ { dhe-rsa-aes-
256-cbc-sha } ] [ { ecdhe-rsa-aes-128-gcm-sha256 } ] [ { ecdhe-rsa-
aes-256-gcm-sha384 } ] | secure-trustpoint | session-cache-timeout } ]
ssl-service-policy <string 1-32> [ { version [ { tls1.0 } ] [ { tls1.1 } ]
[ { tls1.2 } ] | ciphersuite [ { dhe-dss-3des-ede-cbc-sha } ] [ { rsa-
3des-ede-cbc-sha } ] [ { rsa-rc4-128-sha } ] [ { rsa-rc4-128-md5 } ]
[ { rsa-export-rc4-40-md5 } ] [ { rsa-aes-128-cbc-sha } ] [ { rsa-aes-
256-cbc-sha } ] [ { rsa-aes-128-cbc-sha256 } ] [ { rsa-aes-256-cbc-
sha256 } ] [ { dhe-dss-aes-256-cbc-sha } ] [ { dhe-rsa-aes-256-cbc-
sha } ] [ { ecdhe-rsa-aes-128-gcm-sha256 } ] [ { ecdhe-rsa-aes-256-
gcm-sha384 } ] | secure-trustpoint <string 1-32> | session-cache-
timeout <value 60-86400> } ]"

```

Problem Fixed:

Firmware Version	Problems Fixed
V1.00.039	[DBG19040640] The hop count value does not increase 1 when DHCP discover packets relay to DHCP server. (Will Fix in R2) [DBG19040649] The 802.1X RADIUS Statistic are up when the status of server 1 is entering deadtime. (Will Fix in R2) [DBG19050009] The behavior of 802.1X unauthenticated port and authenticated port are abnormal. (Will Fix in R2) [DBG19040521] IGMP Snooping web button error. (Will Fix in R2) [DBG19040443] Deleting specific VLANs will show success but it does not exist in VLAN entries. (Will Fix in R2) [DBG19040181, DBG19040204] Reserved Multicast addresses packets will be captured at the receiver more than sender. (Will Fix in R2) [DBG19040355] DUT will not reply ping packet with jumbo frame. (Will Fix in R2) [DBG19040523] There is no warning message for un-existed time profile on Power Saving page. (Will Fix in R2) [DBG19040533] DUT cannot recognize some IPCams(D-link/Hikvision/Dahua) (Will Fix in R2) [DBG19040520] DUT will mirror few packets under full packet rate. (SW RD will improve on R2)
V1.00.040	Fixed the fan LED error issue
V2.01.006	- The Packets will not be mirrored when the packets meet the ACL deny rule. [DBG19040640] The hop count value does not increase 1 when DHCP discover packets relay to DHCP server. [DBG19040649] The 802.1X RADIUS Statistic are up when the status of server 1 is entering deadtime. [DBG19050009] The behavior of 802.1X unauthenticated port and authenticated port are abnormal. [DBG19040521] IGMP Snooping web button error. [DBG19040181, DBG19040204] Reserved Multicast addresses packets will be captured at the receiver more than sender. [DBG19040355] DUT will not reply ping packet with jumbo frame. [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.

	- The year range changed from "2000-2099" to "2000-2069". Copyright year changed from 2020 to 2021 - Device Information page for removing FLASH which will be not support by Chrome. - Web to Disabled "textbox" while "UDF" selected as "None" in "DHCPv6 Relay Global Settings" page - Modify Introduction string in "DHCP Auto Configuration" page - Remove "Distance/Metric" column on IPv4 route & IPv6 route web page and CLI show IPv4 route & show IPv6 route command.
V2.03.004	Fixed the following problems from OBUs: - Voice VLAN issue. Switch always sends LLDP packet with tag VLAN1 to IP phone. However, it should be untagged packet. [DI20210420000001-Australia] - The switch does not load DHCP Snooping binding entries automatically. DGS-1250 cannot obtain the dhchsnoop database from TFTP server when reboot. Issue happened in some PC, and the PC running TFTP server is directly connected to DGS-1250. [DI20201113000004-Australia] - LACP Irregularities. Link aggregation works incorrect. The ports LACP status could not be bnd1. [DUSA20210331000001-USA] - Switch crashes when pulling the power mid boot up corrupting the firmware. Device fails to boot, and all LEDs light up. If the device connects to console cable, the boot stops at "Please wait for loading. "[DUSA20201126000001-USA] - Drops PoE on all Ports. The device sometimes stopped supply power to all ports. In addition, the device failed to Ping with the peer device via 802.1Q trunk. [DI20210505000001-Australia]
V2.04.003	Fixed the following issues: - Fixed IMPB loose mode is not working properly issue. - Fixed field issue, log "Configuration saved to flash" will display incorrect. [DGC20221122000001-Taiwan] - Fixed field issue, Switch reboot during VAPT scan [IMA20221006000003-India] - Fixed field issue, SNMP outputs disagree. [DEUR20220908000005-UKI] - Fixed field issue, When NIC HOL is triggered, related counter is not recovered, which results in packets cannot be dequeued from that queue. [DRU20211124000001-Russia] - Fixed field issue, DHCP Snooping forwards DHCP packets to LAC other

	member ports [DUSA20220201000005-USA] - Fixed field issue, missing or duplicate logs during reboot. - Fixed field issue, SSH lock up [DUSA20210222000001-USA] - Fixed field issue, the Japanese UI Translation issue [DI20210929000002-Japan] - Fixed field issue, the log entries appeared "Usage threshold 99" message. (DRU20210909000003-DRU) - Support new PoE chipset. - Fix issue where frame size 1522 with tagged packets would be treated as Giants
V2.04.B006	Fixed the following issues (DUSA20230201000001 – DUSA): - When DGS-1250 receives 64 Bytes Tag packet, the Undersize and Runt counter increase in RX port. - When 64 Bytes Tag packet is transmitted via a tag port, the Xmit-err counter increase in TX port. - If jumbo frame is enabled (by max-rcv-frame-size command) and sent jumbo frame, the Xmit-err counter increase in TX port. - A frame size 1522 bytes with tagged packets would be treated as Giants. A frame size 12288 bytes with tagged packets and jumbo frame enable, the error counter "Giants" was incremented. The following is 2.04B006 test cases and results: Result: NO error count. - Frame size 64 bytes <u>with tagged</u>. - Frame size 1522 bytes <u>with tagged</u>. - Frame size 12288 bytes (DGS-1250 Max. Jumbo frame size) <u>with tagged</u> and the jumbo frame enabled. The "rxOversizedPkts" counter was incremented. Result: Error count incremented. - Frame size 12288 bytes <u>with tagged</u> and the jumbo frame disabled (default) The error counter "Giant" was incremented. The "rxOversizedPkts" counter was incremented. The "rxMTUDropPkts" counter was incremented. - Frame size 60 bytes with tagged. The error counter "Rcv-err" was increased. The error counter "Runt" was increased The "rxUndersizedPkts" counter was incremented.
V2.04.P004	[DGC20221023000001] Fake loop detection [DUSA20230201000001] Customer seeing high Runt/Undersize/Xmit-Err counters [HQ20230203000013] The cable diagnostic test results cannot show the

	current status 4. [DBG22110033] IMPB loose mode is not working properly in specific situations 5. [DBG23050041] Unable to access DUT's CLI after using SNMP set AAA auth OIDs.
2.10.004	[DBG23050415] [DGS-1250-28XMP v2.04.003]After enable IPSG+IMPB, traffic can not be forwarded, it seems that IPSG+IMPB can not be cleared completely by command: clear running-config. [DBG23050131] [DGS-1250][2.04.P003][AAA]Acct-session ID always keep same ID number even though changing the different sessions. [DBG23050092] [Reset][WebUI]Reset(excludes the IP address) will clear the IPv6 address. [HQ20221024000001] Case Reopen DGC20220221000004 About DGS-1250 fake loopdetection issue[DGC20221023000001-Taiwan] [HQ20230223000007] DGS-1250 PoE can't working after a period .Please help solve this issue ASAP [DGC20230223000001] [HQ20230208000005] Customer seeing high Runt/Undersize/Xmit-Err counters on the ports of his DGS-1250-52XMP switches[DUSA20230201000001-USA] [HQ20230203000013] The cable diagnostic test results cannot show the current status. [HQ20230417000007] [VLAN Interface Information issue for DGS-1250 with FW 2.03.B011[DEUR20230417000001-South Europe]] [HQ20230322000009] [What is the correct behavior when set storm control level kbps to 1?] [HQ20230717000003] Customer reporting Password-Encryption error on DGS-1250 series[Refer_to_DUSA20230715000001]] [HQ20230523000010] DGS-1250 series currently experiences a situation of management disconnection[DGC20230523000001-Taiwan] [HQ20230619000004] DGS-1250 show cable-diagnostics value are not correct issue[DGC20230618000001-Taiwan] [HQ20231023000004] DI20231023000002 [DGS-1250/2.03] doesn't show an error message in "no snmp-server comm" under being used. - Black box vulnerability: R2.04.003 PS-409 vulnerability fix(include Openssl upgrade to at least ""1.1.1l"" or latest version) - OnSec-TC-03014001(Known Vulnerability Testing) - OnSec-TC-03011002(SSH Weak Cipher Algorithm)

	- OnSec-TC-09002004 - OnSec-TC-09002010 - OnSec-TC-09006012 - OnSec-TC-09002002 - SNR-20211125-002(SSH Weak Algorithms) - SNR-20220119-001(New ciphers for SSH)"
2.10.05	1. DBG24040285: Enable the DGS-1250 to support importing certificate and private key files that are password-protected. 2. DBG24040256: DGS-1250 2.10.004 failed to test case DKP1705026-0017 - "IPv6 Source Guard_IPv6SG and Flow control test".

* D-Link tracking number is enclosed in []

Known Issues:

Firmware Version	Issues	Workaround
V1.00.039	N/A	
V1.00.004	N/A	
V2.01.006	[DBG19040443] Deleting specific VLANs will show success but it does not exist in VLAN entries. [DBG19040523] There is no warning message for un-existed time profile on Power Saving page. Chip Limitation: - 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. - 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. - Dynamic ARP entries cannot be kept when the related L2 entry age-out - 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 V2.03.004	Chip Limitation: - 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. - Dynamic ARP entries cannot be kept when the related L2 entry age-out - 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.	
V2.04.P004	[DBG23050180] Vulnerabilities found from black box test	Fix in next version.
	[DBG23050092] Reset(excludes the IP address) will clear the IPv6 address.	Fix in next version.
	[DBG23050131] [AAA]Acct-session ID always keep same ID number even though changing the different sessions.	Fix in next version.
V2.10.005	1. Reserved destination IP 239.*.*.*, 224.0.0.*, and 224.0.1.*, IPv6 FF0*::*.*, and FF0*::DB8:0:0 cannot be filtered on Filter Unregistered Mode. 2. Vulnerability Issue a. Known Vulnerability Testing (OnSec-TC-03014001) b. SSH Weak Cipher Algorithm (OnSec-TC-03011002) c. 3DES Algorithm Testing (OnSec-TC-09002004) d. CBC Mode Algorithm Testing (OnSec-TC-09002010) e. RC4 Algorithm Testing (OnSec-TC-09002002) TLSv1/SSLv3 Renegotiation Vulnerability (OnSec-TC-09006007) f. Suggestion: Disable below weak SSH Algorithms: ° Encryption Algorithms [aes128-ctr] [aes192-ctr] [aes256-ctr] [3des-cbc] [blowfish-cbc] [twofish128-cbc] [twofish192-cbc] [twofish256-cbc] [twofish-cbc] [arcfour]	Fix in next version.

[cast128-cbc]
[aes128-ctr]
[aes192-ctr]
[aes256-ctr]
° MAC Algorithms
[hmac-sha1]
[hmac-sha1-96]
[hmac-md5]
[hmac-md5-96]
° Hostkey Algorithms
[ssh-dss]
° Key Exchange Algorithms
[diffie-hellman-group14-sha1]
[diffie-hellman-group1-sha1]
[diffie-hellman-group-exchange-sha1]
[ecdh-sha2-nistp256]
[ecdh-sha2-nistp384]
[ecdh-sha2-nistp521]
[curve25519-sha256]
Disable below weak TLS Versions:
[TLS 1.0]
[TLS 1.1]
Disable below weak TLS Ciphers:
[DHE_DSS_WITH_3DES_EDE_CBC_SHA]
[RSA_WITH_3DES_EDE_CBC_SHA]
[RSA_EXPORT_WITH_RC4_40_MD5]
[RSA_WITH_RC4_128_MD5]
[RSA_WITH_AES_128_CBC_SHA]
[RSA_WITH_AES_256_CBC_SHA]
[DHE_DSS_WITH_AES_256_CBC_SHA]
[DHE_RSA_WITH_AES_256_CBC_SHA]

Related Documentation:

- DGS-1250 Series_A1 A2 CLI Manual_v2.04(US)
- DGS-1250 Series_A1_HW Installation Guide_v2.03(WW)
- DGS-1250 Series_A1_Web UI Manual_v2.03(WW)
- DGS-1250 Series_A1_Getting Started Guide(WW)