
**Firmware Version:** V1.60.012
**Prom Code Version:** V1.00.016
**Published:** 2018/11/5

---

These release notes include important information about D-Link DGS-1510 Series firmware revisions. Please verify that these release notes are correct for your switch:

- If you are installing a new switch, please check the hardware version on the device label; make sure that your switch meets the system requirement of this firmware version. Please refer to Revision History and System Requirement for detailed firmware and hardware matrix.
- If the switch is powered on, you can check the hardware version by typing "show system" command or by checking the device information page on the web graphic user interface.
- If you plan to upgrade to the new firmware release, please refer to the Upgrade Instructions:

D-Link switches support firmware upgrade via TFTP server. You can download the firmware from D-Link web site http://tsd.dlink.com.tw, and copy the downloaded firmware to the TFTP server folder. Please make sure that the TFTP server is accessible from the switch via networks.

For more detailed information regarding DGS-1510 Series switch products, please refer to Related Documentation.

You can also download the switch firmware, D-View modules and technical documentation from http://tsd.dlink.com.tw.

**Content:**

## Revision History and System Requirement

| Firmware Version | Date | Model | Hardware Version |
|---|---|---|---|
| Runtime: v1.60.012<br>PROM: v1.00.016 | 2018/11/5 | DGS-1510 | A1/A2 |
| Runtime: v1.50.021<br>PROM: v1.00.015<br>(due to new models addition, DGS-1510-52XMP A1 & DGS-1510-52X A2, no impact to existing models) | 2018/01/12 | DGS-1510 | A1/A2 |
| Runtime: v1.40.019<br>PROM: v1.00.012 | 2017/09/10 | DGS-1510 | A1 |
| Runtime: v1.30.007<br>PROM: v1.00.012 | 2015/10/20 | DGS-1510 | A1 |
| Runtime: v1.20.011<br>PROM: v1.00.012 | 2015/5/2 | DGS-1510 | A1 |
| Runtime: v1.10.005<br>PROM: v1.00.011 | 2014/5/21 | DGS-1510 | A1 |
| Runtime: v1.00.031<br>PROM: v1.00.009 | 2014/1/15 | DGS-1510 | A1 |
| Runtime: v1.00.029<br>PROM: v1.00.009 | 2014/1/13 | DGS-1510 | 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 (RJ-45 console port)**

Connect a workstation to the switch console port and run any terminal program that can emulate a VT-100 terminal. The switch console 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. The default username and password are as below:

Username: **admin**

Password: **admin**

To upgrade the switch firmware, execute the following commands:

| Command | Function |
|---|---|
| copy tftp://*location/filename* flash: *filename* | Download firmware file from the TFTP server to the switch. |
| boot image *URL(filename)* | Change the boot up image file. |
| show boot | Display the information of current boot image and configuration. |
| reboot | Reboot the switch. |

**Example:**

**DGS-1510#**copy tftp: //192.168.0.27/firmware.had flash: run.had

Address of remote host [192.168.0.27]
Source filename [firmware.had]
Destination filename [run.had]
Accessing tftp://192.168.0.27/ firmware.had...
Transmission start...
Transmission finished, file length 5156864 bytes.
Please wait, programming flash... Done

**DGS-1510#**configure terminal
**DGS-1510(config)#**boot image c:/switch-image1.had

**DGS-1510#**show boot

Unit 1
Boot image: /c:/1.20.B014
Boot config: /c:/config.cfg

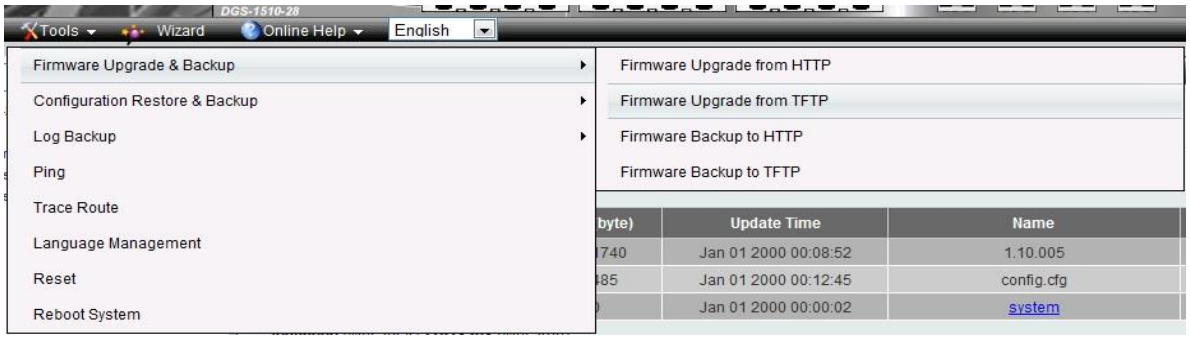
**DGS-1510#**reboot
Are you sure you want to proceed with the system reboot? (y|n) y
Please wait, the switch is rebooting...

**Upgrading by using Web-UI**

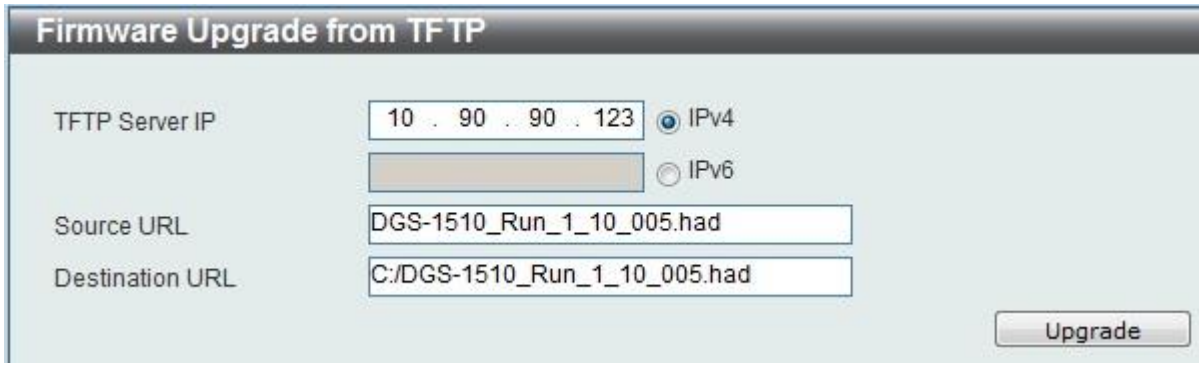
1. Connect a workstation installed with java SE runtime environment to management port of the device and also connect console cable to switch's console port.
2. Open the web browser from the workstation and enter the IP address of the switch. The switch's default IP address is **10.90.90.90**
3. Enter administrator's username and password when prompted. **It should be noted starting from R1.20 formal firmware release the default login settings are as below:**

   **Username: admin**

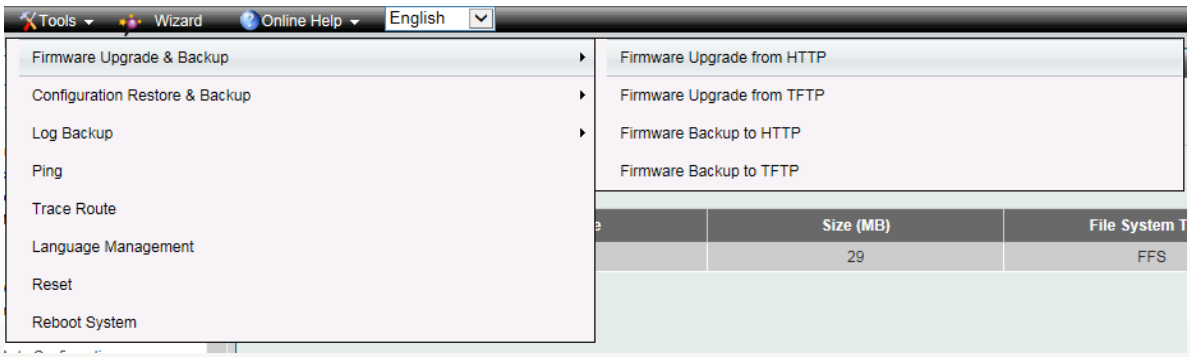
   **Password: admin**
4. To update switch's firmware or configuration file via TFTP, select ***Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP***.



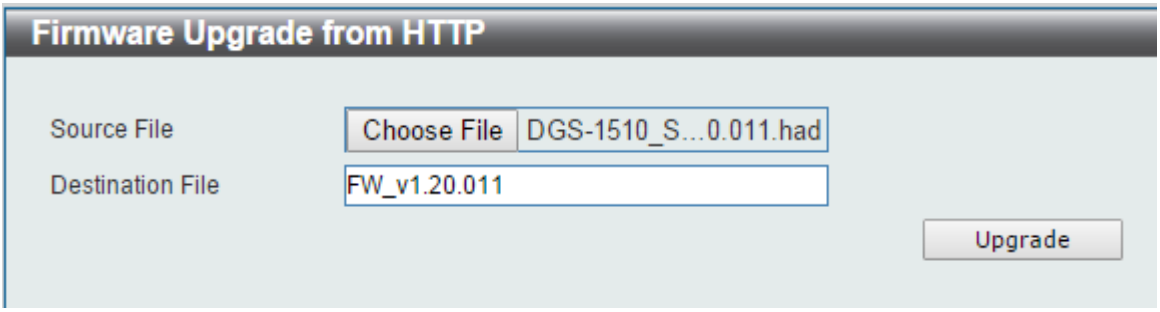

5. Enter the TFTP Server IP address.
6. Enter the name of the firmware file located on the TFTP server.
7. Enter the destination path and the desired file name.
8. Click "***Upgrade***" button.



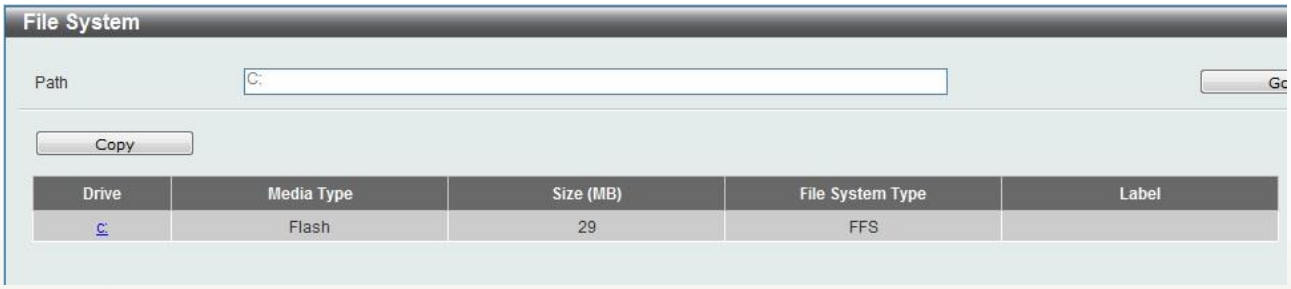

9. Transmission will start and wait until the status is completed by displaying ***100%*** complete.
10. Alternatively, the switch's firmware or configuration file can also be upgraded via HTTP, select ***Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP***.

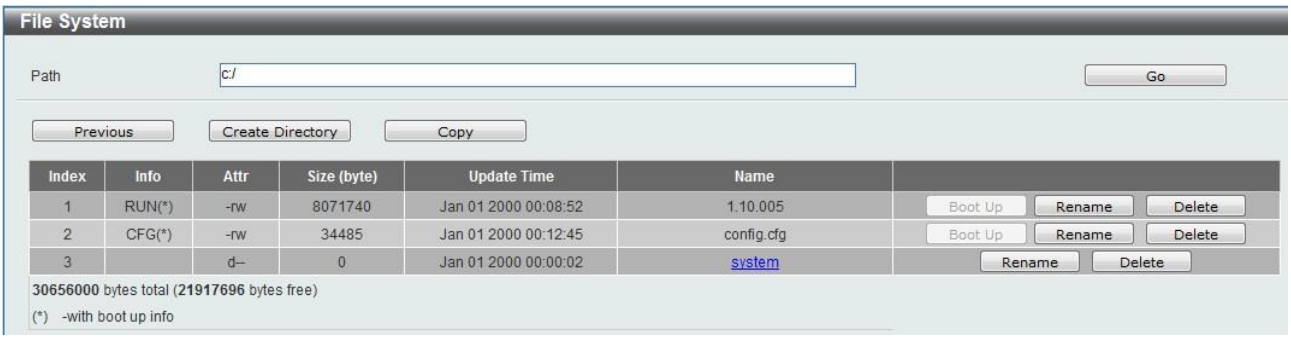



11. Enter the source and destination file.
12. Click "***Upgrade***" button.

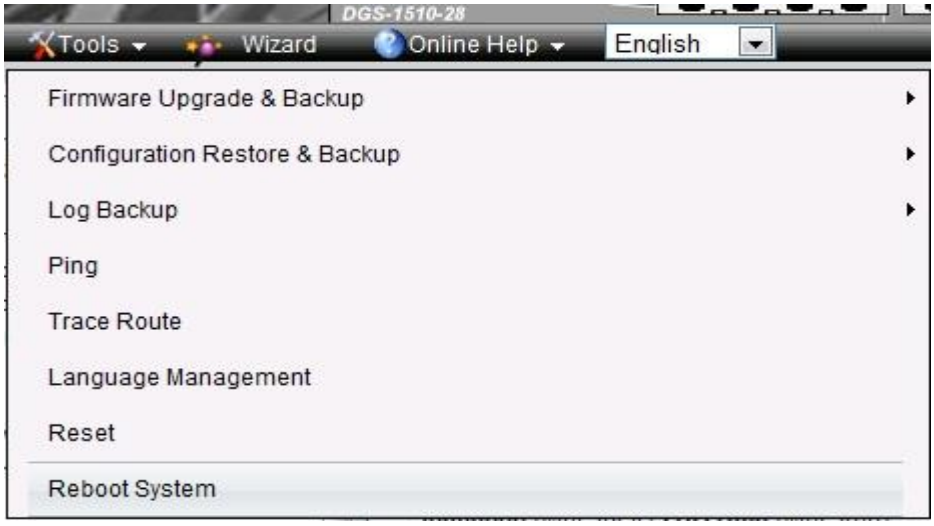



13. Transmission will start and wait until the status is completed by displaying ***100%*** complete.
14. To select the boot up image used for next reboot, click ***Management > Flash System*** in the function tree and then click the ***C:*** drive name. When you see the files list, click corresponding ***Boot Up*** button to specify the firmware that will be used for next and subsequent boot up.




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




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


## New Features

| Firmware Version | New Features |
|---|---|
| V1.60.012 | 1. Changing output's format when executing show running config command<br>2. Removing Java from web page<br>3. Set one boot image on stacked units<br>4. Display slave's information of stacked unit via "show tech-support" command<br>5. IGMP V3 protocol<br>6. "Do" command in EXEC mode<br>7. Configure Secondary IP setting via IPv4 interface in Web UI |
| V1.50.021 | 1. Login Banner<br>2. Exec Banner |

| | |
|---|---|
| | 3. Supports Monitor logging in CLI<br>4. Session timeout (for outgoing remote session)<br>5. "show interface xx description" command in CLI<br>6. Add logging feature for ARP Spoofing Prevention<br>7. Enhance static multicast mac address table from 128 to 256<br>8. Supports SHA-256 for SSH<br>9. Enhance RADIUS Accounting for Command Logging (for TACACS+ accounting ONLY) |
| V1.40.019 | 1. Add UDP helper<br>2. Enhance the show logging output for stacking features<br>3. Enhance priority between IP Source Guard and user-defined ACL<br>4. Change IPv6 Route Advertisement from host to router mode<br>5. Add LBD v4.07<br>6. Add Auto Surveillance VLAN 2.0<br>7. Add stacking MIBs for G2 CLI, swUnitMgmtStartPort,swUnitMgmtPortRange<br>8. Add TLS 1.2<br>9. Enhance CLI for "Show running-config" with output modifiters [effective \| all] [interface INTERFACE-ID]<br>10. Enhanced login page for Web UI to have the "username : admin" being filled in<br>11. Enhance Trap Source Interface in "SNMP Global Setting" page<br>12. Add PD-Alive |
| V1.30.007 | 1. Add a New encryption method based on MD5<br>2. MAC-based VLAN<br>3. Protocol-based VLAN<br>4. Telnet Client (w/o MIB/Web)<br>5. SSH & telnet session timeout behavior change<br>6. Displaying web UI sessions in "show users" command<br>7. VLAN Cloning in web UI<br>8. Auto saving of configuration made from DDP protocol<br>9. Update a new web UI top image |
| V1.20.011 | 1. Add NTP (RFC5905)<br>2. Modify IP interface from 8 to 16<br>3. Modify STP edge default settings to "True"<br>4. Add ERPS<br>5. Add sFlow<br>6. Add default username (admin) & password (admin) |
| V1.10.005 | 1. Existing 4 models can now Physical Stack with 2 new members (DGS-1510-28X & DGS-1510-52X)<br>2. Add BPDU Attack Protection<br>3. Add the Command "Trace route"<br>4. Add the Command "prompt" for customizing CLI prompt<br>5. Add "Login Method" page for Web UI (for telnet session setup requirements under Web UI)<br>6. Supports D-Link's new IP Cameras' MAC Address ranges: B0:C5:54:00:00:00 ~ B0:C5:54:7F:FF:FF for Auto Surveillance VLAN<br>7. Modify user-defined OUI of Auto Surveillance VLAN & Auto Voice VLAN from 5 to 10<br>8. Modify web-UI's smart wizard to include a last step for configuring username & password |
| V1.00.031 | None |
| V1.00.029 | First release, please refer to datasheet and manual for detail function support |

## Changes of MIB & D-View Module

The new features of MIB file are also included in the corresponding D-View module. Please download the D-View module on http://tsd.dlink.com.tw. For detailed changes of MIB content, please refer to the modification history in each MIB file.

| Firmware Version | MIB File |
|---|---|
| V1.60.012 | Update the following MIBs:<br>1. DLINKSW-IPMCAST-EXT-MIB.mib<br>2. DLINKSW-NETWORK-PROTOCOL-PORT-PROTECT.mib |
| V1.50.021 | Update the following MIBs:<br>1. DLINKSW-SYSLOG-MIB.mib<br>2. DLINKSW-ASP-MIB.mib<br>3. DLINKSW-SURVEILLANCE-VLAN-MIB<br>4. SWDGS1510PRIMGMT-MIB |
| V1.40.019 | Modify the below MIBs:<br>1. DLINKSW-STACK-MIB.mib<br>2. DLINKSW-SSL-MIB.mib<br>3. DLINKSW-IP-EXT-MIB.mib<br>4. DLINKSW-ACL-MIB.mib<br>5. IP-MIB.mib<br>6. DLINKSW-SURVEILLANCE-VLAN-MIB.mib<br>7. DLINKSW-POE-MIB.mib |
| V1.30.007 | 1. Add new feature UDP helper in D-View<br>2. Add new feature MAC Based VLAN in D-View<br>3. Add new feature Protocol Based VLAN in D-View |
| V1.20.011 | 1. Add DLINKSW-SFLOW-MIB<br>2. Add DLINKSW-ERPS-MIB<br>3. Add DLINKSW-NTP-MIB |
| V1.10.005 | 1. Add DLINKSW-BPDU-PROTECTION-MIB.mib<br>2. Add DISMAN-TRACEROUTE-MIB.mib<br>3. Modify DGS-1510 Series Physical Stacking for 6 models in D-View (2 new models DGS-1510-28X, DGS-1510-52X)<br>4. Add new features BPDU Protection in D-View<br>5. Add new features Trace Route in D-View |
| V1.00.031 | None |
| V1.00.029 | First release, please refer to datasheet for detail MIB support |

## 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 |
|---|---|
| V1.60.012 | **1. Network Protocol Port Protect**<br>network-protocol-port protect {tcp \| udp}<br>no network-protocol-port protect {tcp \| udp}<br>show network-protocol-port protect<br><br>**2. IP Multicasting**<br>ip multicast table-lookup-mode { ip \| mac}<br>no ip multicast table-lookup-mode<br>show ip multicast<br><br>**3. Boot image command**<br>boot image [check] [all] URL<br><br>**4. Tech Support command**<br>show tech-support [unit UNIT-ID]<br>debug show tech-support [unit UNIT-ID]<br><br>**5. Do Command**<br>do COMMAND |
| V1.50.021 | 1. "**show interface xx description**" command in CLI:<br>show interfaces [INTERFACE-ID [,\|-] ] description |
| V1.40.019 | 1. **LBD**<br>loopback-detection address-type { multicast \| broadcast }<br>no loopback-detection address-type<br><br>2. **Surveillance VLAN**<br>surveillance vlan onvif-discover-port <value 554, 1025-65535><br>no surveillance vlan onvif-discover-port<br>surveillance vlan onvif-ipc IP-ADDRESS state {enable \| disable}<br>no surveillance vlan onvif-ipc IP-ADDRESS state<br>surveillance vlan onvif-ipc IP-ADDRESS description TEXT<br>no surveillance vlan onvif-ipc IP-ADDRESS description<br>surveillance vlan onvif-nvr IP-ADDRESS description TEXT<br>no surveillance vlan onvif-nvr IP-ADDRESS description<br>show surveillance vlan onvif-ipc interface [ INTERFACE-ID [, \| -] ] {brief \| detail }<br>show surveillance vlan onvif-nvr interface [ INTERFACE-ID [, \| -] ] [ipc-list]<br><br>3. **UDP helper**<br>ip helper-address IP-ADDRESS<br>no ip helper-address [ IP-ADDRESS ]<br>ip forward-protocol udp [PORT]<br>no ip forward-protocol udp [PORT]<br>show ip helper-address [INTERFACE-ID]<br>show ip forward-protocol udp<br><br>4. **ACL**<br>Add "vlan-range MIN-VID MAX-VID" option<br><br>5. **TSL 1.2**<br>ssl-service-policy POLICY-NAME<br>[version [ssl3.0] [tls1.0] [tls1.1] [tls1.2] ] \|<br>[ ciphersuite<br>[dhe-dss-3des-ede-cbc-sha] |

| | |
|---|---|
| | [rsa-3des-ede-cbc-sha]<br>[rsa-rc4-128-sha]<br>[rsa-rc4-128-md5]<br>[rsa-export-rc4-40-md5]<br>[rsa-aes-128-cbc-sha]<br>[rsa-aes-256-cbc-sha]<br>[rsa-aes-128-cbc-sha256]<br>[rsa-aes-256-cbc-sha256]<br>[dhe-dss-aes-256-cbc-sha]<br>[dhe-rsa-aes-256-cbc-sha] ] \|<br>secure-trustpoint TRUSTPOINT \|<br>session-cache-timeout TIME-OUT ]<br><br>no ssl-service-policy POLICY-NAME<br>[version [ssl3.0] [tls1.0] [tls1.1] [tls1.2] ] \|<br>[ ciphersuite<br>[dhe-dss-3des-ede-cbc-sha]<br>[rsa-3des-ede-cbc-sha]<br>[rsa-rc4-128-sha]<br>[rsa-rc4-128-md5]<br>[rsa-export-rc4-40-md5]<br>[rsa-aes-128-cbc-sha]<br>[rsa-aes-256-cbc-sha]<br>[rsa-aes-128-cbc-sha256]<br>[rsa-aes-256-cbc-sha256]<br>[dhe-dss-aes-256-cbc-sha]<br>[dhe-rsa-aes-256-cbc-sha] ] \|<br><br>6. **SNMP**<br>no snmp-server host {<IP-ADDRESS> \| <IPV6-ADDRESS> }<br>[<community-name>] |
| V1.30.007 | **New encryption method based on MD5**<br>1. username NAME [privilege LEVEL] [nopassword \| password [0 \| 7 \| 15 ] PASSWORD]<br>2. enable password [level PRIVILEGE-LEVEL] [0\| 7 \| 15 ] PASSWORD<br>3. service password-encryption [ 7 \| 15 ]<br><br>**Telnet Client (w/o MIB/Web)**<br>1. telnet [IP-ADDRESS \| IPV6-ADDRESS \| Domain Name ] [TCP-PORT]<br><br>**Displaying web UI sessions in "show users" command**<br>1. clear line LINE-ID |
| V1.20.011 | None |
| V1.10.005 | None |
| V1.00.031 | None |
| V1.00.029 | First release |

## Problem Fixed

| Firmware Version | Problems |
|---|---|
| V1.60.012 | 1. Fixed http secure server bug of not synchronizing properly (DI20171204000001-Japan)<br>2. Fixed Secondary IP interface is not being shown when configured (DI20180418000003, DI20171129000004-Japan)<br>3. Fixed memory overflow bug on ARP aging-time feature (DI20171130000004-Japan)<br>4. Fixed STP & LBD bug, which is able to enable in the same port (DI20171218000002, DI20180418000006-Japan)<br>5. Fixed SNTP syntax error in Web UI (DI20180222000004, DI20180418000004-Japan)<br>6. Fixed CLI charset default to ASCII (DI20180213000003, DI20180418000005-Japan)<br>7. Fixed UDP BLAT attack function missing from DoS feature (DI20180223000004, DI20180419000001-Japan)<br>8. Fixed Web UI syntax error under Traditional Chinese (DGC20180227000001-Taiwan)<br>9. Fixed LLDP-MED bug where its setting is missing in the output of "show run configuration" (DRU20180306000001-Russia)<br>10. Fixed DGS-1510-52XMP's Fan & PoE bug issues (DEUR20180228000005, DEUR20180201000003-Europe)<br>11. Fixed time zone format to function seamlessly with DNA (DI20180131000002-Australia)<br>12. Fixed trace route TTL error bug (DEUR20180329000001-Europe)<br>13. Fixed web UI "save configuration" bug issue (DEUR20180403000007-Europe)<br>14. Fixed CLI command listing displayed in descending order instead of ascending (DI20180528000003-Japan)<br>15. Fixed command "debug copy tech-support" bug issue (DI20180522000002-Japan)<br>16. Modified the behavior to include 'clear port description' via checkbox in web UI (DRU20180529000004-Russia) |

| | |
|---|---|
| | 17. Fixed translation error in Italian (DEUR20180531000005-Europe)<br>18. Fixed SNMP server source interface priority error bug (DI20180524000003-Japan)<br>19. Fixed Voice VLAN & LLDP-MED bug issue (DRU20180409000002-Russia)<br>20. Fixed "VLAN interface" setting's bug in web UI (DI20180606000003-Japan)<br>21. Fixed session timeout bug of not timing out & shut session after preset time is exceeded (DEUR20180709000001-Europe)<br>22. Fixed default admin account re-appearance bug after it was deleted (DUSA20180726000003-USA)<br>23. Enhance the feature of clone VLAN as well as to support cloning cross units under physical stacking environment (DRU20180806000002-Russia)<br>24. Fixed coding/programming errors in RADIUS (DI20180803000001-Australia)<br>25. Fixed & enhanced auto-negotiation issue (DI20170203000004, DI20180302000008-Japan)<br>26. Fixed IP source guard bug issue (DGC20171121000001-Taiwan)<br>27. Fixed SNMPv6 response time bug issue (DGC20180619000001-Taiwan)<br>28. Fixed DHCP Snooping bug issue (DRU20180830000002-Russia)<br>29. Fixed IPv6 coding error bug issue (DGC20180903000001-Taiwan) |
| V1.50.021 | 1. Fixed IPv6 header bug when receiving icmpv6 requests with hop by hop option (DGC20170628000001-Taiwan)<br>2. Fixed IGMP Snooping bug which freezes the switch (DEUR20170814000001-DEUR, DEUR20170912000003-DEUR)<br>3. Fixed software bug for showing the wrong DDM information via SNMP (DRU20170907000003-Russia)<br>4. Fixed firmware's file size display bug between master and slave (physical stacking) when it is upgraded via D-View7 (DI20170915000002-DJP)<br>5. Fixed DHCP Client bug which caused SSH session to stop functioning (DLA20171011000001-DLA)<br>6. Fixed DHCP snooping bug when PC's IP address is altered between Static and DHCP (DGC20171121000001-Taiwan) |
| V1.40.019 | 1. Fixed some SNMP bugs issue. (DI20150907000007-DJP)<br>2. Fixed physical stacking bug where master's configuration was overwritten by slave unit (DI20151014000001-DJP) |

3. Fixed physical stacking bug when master unit is down, flags on slave and backup master were not updated (DI20151111000001-DJP)
4. Fixed the bug to protect memory allocation to prevent allocated memory blocks from overlapping (DI20151221000005-DJP)
5. Fixed VLAN option 'replace' being accidently removed from Web UI by software R&D. (DEUR20160530000001-DEUR)
6. Fixed ERPS and LAG software bug when they are both enabled via WebUI. (DEUR20160427000005-DEUR)
7. Fixed sFlow bug not getting a system interface address when interface vlan1 doesn't exist (DRU20160201000001-DRU)
8. Fixed javascript error bug on html for webUI (DEUR20160921000004-DEUR)
9. Fixed some bugs on ACL rules (DI20151019000004-DJP)
10. Fixed webUI's webpage bug (DEUR20170511000002-DEUR)
11. Fixed ERPS ring's bug when 2 switches are rebooted (DEUR20170516000004-DEUR)
12. Fixed CPU's Ingress Backpressure (IBP) limitation by enlarging its IBP threshold (DEUR20170301000006-DEUR)
13. Fixed some bug issues related to:
14. Difference between running-config and startup-config.
15. ERPS blank profile cannot be removed.
16. ERPS won't be in idle status if it is applied with a blank profile.
17. (DI20151124000002-DJP, DI20170201000004-DJP)
18. Fixed a SSH security bug (DRU20170120000003-DRU)
19. Fixed NTP DDOS vulnerability issues (DGC20170704000001-DTW)
20. Fixed CPU utilization deficiencies in Web UI, related to case (DRU20150818000002-DRU)
21. Fixed Web UI javascript bug which affected SNMP settings (DRU20151109000002-DRU)
22. Fixed DHCP Server Screening implementation to limit the global server number to 5 (DGC20150914000005-DTW)
23. Fixed LBD bug being trapped at CPU without processing (DGC20150828000002-DTW)
24. Fixed IP addresses' bug for endian formatting (DGC20151019000002-DTW)
25. Fixed MAC Authentication CLI bug (DRU20151102000005-DRU)

| | |
|---|---|
| | 26. Fixed group name mismatch bug in MIB (DI20151104000006-DJP)<br>27. Fixed default VLAN ip address display in Web UI (DGC20151109000001-DTW)<br>28. Fixed QoS' meter max rate bug (DEUR20151124000011-DEUR)<br>29. Fixed IP addresses' endian formatting bug when using TFTP server to upload configuration (DRU20151221000003-DRU)<br>30. Fixed physical stacking bug when f/w upgrading is not propagated properly to slaves (DUSA20151203000001-DUSA)<br>31. Fixed software coding bug related to physical stacking and web UI's features (DEUR20160617000002-DEUR)<br>32. Fixed Radius bug for retrieving wrong IP address (DRU20160728000001-DRU)<br>33. TLS 1.2 issues, which is not supported on older f/w. This feature is added in this version (DEUR20160920000003-DEUR)<br>34. Fixed Web UI's HTML coding error (DEUR20170124000001-DEUR) |
| V1.30.007 | 1. PoE related software issues are fixed. (DEUR20141105000002-EU, DEUR20141001000006-EU, DUSA20150304000002-USA, DEUR20141119000001-EU, DRU20141212000001-Russia, DGC20150302000001-Taiwan)<br>2. Switch hung up due to chipsets vendor's SDK with wrong definitions. (DGC20150122000001-Taiwan)<br>3. Fatal error discovered due to chipsets vendor's SDK with wrong definitions. (DI20141216000001-Japan)<br>4. Software bug caused physical stacking to malfunction. (DI20150127000004-Japan)<br>5. Modified software to limit ARP request to CPU at 64Kbps, due to customer's environment with many ARP requests.(DEUR20150224000002-UKI)<br>6. Resolved the bug where IP address of device information are not updated and synced. (DI20150313000002-Japan)<br>7. Packet buffer draining issue, Software R&D enhance code to prevent it from happening. (DI20150610000004-Japan) |
| V1.20.011 | 1. Modified DHCP Snooping's default value of "per VLAN disabled" to "per VLAN enable" to allow PCs to get IP address via DHCP on a stacking member port's VLAN. (DI20140411000011-Japan)<br>2. Fixed BPDU bug that caused looping when STP blocking port was changed |

| | |
|---|---|
| | between stacking units.(DI20140428000007-Japan)<br>3. Fixed BPDU bug that caused looping when MSTP blocking port was changed between stacking units.( DI20140526000003 & DI20140619000008-Japan)<br>4. Fixed the SSH RSA/DSA key generated in stacking master switch which doesn't sync to its slave switches. (DI20140604000001-Japan)<br>5. Fixed IP address shown in reverse in log when saving configuration via SNMP. (DRU20140512000002-Russia)<br>6. Fixed CPU interrupt sensitivity software settings that caused the switch to either hung up or lost management respectively. (DEUR20140929000001-EU & DUSA20150325000004-USA)<br>7. Fixed the switch from entering exception mode when a port is being linked up during MAC authentication. (DGC20140715000003-Taiwan)<br>8. Fixed IPv6 JWAC bug that did not redirect to authentication page if the interface's IPv6 state is disabled or no IPv6 address has been assigned. DI20140722000002-Japan)<br>9. Modify software settings in order for Realtek 8111R NIC card to retrieve IP address from DHCP server faster while transiting via DGS-1510. (DGC20140717000005-China)<br>10. Enhance support for Intel 82579 NIC card using different driver versions so those DHCP bootp packets are not dropped. (DEUR20140311000007-EU)<br>11. Fixed DHCP Relay bug that caused PCs not able to get IP address from DHCP server when client & server are in the same VLAN. (DEUR20140902000001-EU)<br>12. Fixed incorrect VLAN Link status information shown in CLI. (DRU20141203000001-Russia)<br>13. Fixed the bug of not accepting DHCP relay source address using subnetted network address. DGC20141213000001-Taiwan)<br>14. Fixed the bug of not accepting configuring switch interface using subnetted network address.(DRU20141218000001-Russia) |
| V1.10.005 | 1. DHCP Snooping blocked packets from a VLAN which was not enabled by DHCP Snooping. (DI20140402000002-Japan)<br>2. Modify the minimum value of command "storm-control unicast level" from 1 to 0. (DI20140325000011-Japan)<br>3. When DHCP Relay is enabled on a VLAN, DGS-1510 still forward DHCP |

| | |
|---|---|
| | broadcast packets to the port connected to DHCP server. (DGC20140113000001-China) |
| V1.00.031 | 1. Fixed switch rebooting issue in first firmware release. Please see known issues for details.<br>2. Fixed the safeguard engine bug in first firmware release. Please see known issues for details. |
| V1.00.029 | First release |

* D-Link tracking number is enclosed in ()

## Known Issues

| Firmware Version | Issues | Workaround |
|---|---|---|
| V1.60.012 | None | |
| V1.50.021 | None | |
| V1.40.019 | None | |
| V1.30.007 | None | |
| V1.20.011 | 1. Switch PoE function will stop delivering power after a while, these are reported in:<br>DEUR20141105000002-EU<br>DEUR20141001000006-EU<br>DUSA20150304000002-USA<br>DEUR20141119000001-EU<br>DRU20141212000001-Russia<br>DGC20150302000001-Taiwan | It is highly recommended (DGS-1510-28P & DGS-1510-28XMP) to avoid using this firmware. Please kindly contact HQ's Tech Support or PP to get a beta firmware fix, **R1.20.B013** that had fixed this issue.<br>R&D fixed this software bug in PoE's Microcontroller settings |
| V1.10.005 | 2. After creating a new Access List profile either via CLI or Web UI, the edit button under Access-List was not greyed out in D-View.<br>Per D-View's design SPEC, this is prohibited.<br>3. IP Source Guard Static Binding table list is created either from CLI or Web UI; it was not editable from D-View. This is a bug. | These are software bugs of D-View module; they will be fixed in the next version. |
| V1.00.031 | None | |

| | | |
|---|---|---|
| V1.00.029 | 1. Under the below scenario, DGS-1510 will reboot: When a switch port (DGS-1510) is set as auto-negotiation, the other connected switch is hardcoded with 100Mbps speed. Then perform cable diagnostic on DGS-1510 and do a "show cable-diagnostic", the switch will reboot.<br>2. When issuing save configuration command, safeguard engine may trigger. | This is a bug, will be fixed in firmware version 1.00.031. |

* D-Link tracking number is enclosed in ()

## Related Documentation

- DGS-1510 Series Web UI Reference Guide Release
- DGS-1510 Series CLI Reference Guide Release
- DGS-1510 Series HW Installation Guide Release