



Firmware Version: 2.51.B022
Boot Code Version: 1.00.017
MIB Version: 2.50.002
D-View Module Version: 1.0.0.7
Published: Apr. 09, 2018

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:	2
Upgrade Instructions:	3
Upgrade using CLI (via Telnet).....	4
Upgrade using Web-UI.....	4
New Features:.....	4
Changes in MIB & D-View Modules:	7
Changes in Command Line Interface:.....	10
Problem Fixed:	11
Known Issues:	12
Related Documentation:	13

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
Runtime: v2.51.B022 Boot: 1.00.017	09-Apr.-18	DGS-1500-20	A2
Runtime: v2.51.B021 Boot: 1.00.017	18-Sep.-17	DGS-1500-20	A2
Runtime: v2.51.B019 Boot: 1.00.017	26-Jan.-16	DGS-1500-20	A2
Runtime: v2.51.B018 Boot: 1.00.017	15-Jan.-16	DGS-1500-20	A2
Runtime: v2.51.B017 Boot: 1.00.017	14-Dec.-15	DGS-1500-20	A2
Runtime: v2.51.B016 Boot: 1.00.017	26-Aug.-15	DGS-1500-20	A2
Runtime: v2.51.015 Boot: 1.00.017	25-Feb.-15	DGS-1500-20	A2
Runtime: v2.51.014 Boot: 1.00.017	13-Feb.-15	DGS-1500-20	A2
Runtime: v2.51.B011 Boot: 1.00.017	30-Jan.-15	DGS-1500-20	A2
Runtime: v2.51.B010 Boot: 1.00.017	27-Nov.-14	DGS-1500-20	A2
Runtime: v2.51.B009 Boot: 1.00.017	07-Nov.-14	DGS-1500-20	A2
Runtime: v2.51.B008 Boot: 1.00.017	28-Oct.-14	DGS-1500-20	A2
Runtime: v2.51.B008 Boot: 1.00.016	19-Sep.-14	DGS-1500-20	A2
Runtime: v2.51.B007 Boot: 1.00.015	25-Aug.-14	DGS-1500-20	A2
Runtime: v2.51.B006 Boot: 1.00.015	21-July-14	DGS-1500-20	A2
Runtime: v2.51.005 Boot: 1.00.015	26-May-14	DGS-1500-20	A2

Runtime: v2.51.B002 Boot: 1.00.013	22-Apr.-14	DGS-1500-20	A1
Runtime: v2.50.B009 Boot: 1.00.013	14-Feb.-14	DGS-1500-20	A1
Runtime: v2.50.008 Boot: 1.00.013	31-Dec.-13	DGS-1500-20	A1
Runtime: v2.50.B004 Boot: 1.00.013	13-Dec.-13	DGS-1500-20	A1
Runtime: v2.50.003 Boot: 1.00.013	09-Dec.-13	DGS-1500-20	A1
Runtime: v2.50.B002 Boot: 1.00.013	09-Dec.-13	DGS-1500-20	A1
Runtime: v2.50.B001 Boot: 1.00.013	22-Nov.-13	DGS-1500-20	A1
Runtime: v2.10.B020 Boot: 1.00.013	01-Nov.-13	DGS-1500-20	A1
Runtime: v2.10.B019 Boot: 1.00.013	20-Aug.-13	DGS-1500-20	A1
Runtime: v2.10.002 Boot: 1.00.013	08-Nov.-12	DGS-1500-20	A1
Runtime: v2.00.015 Boot: 1.00.013	15-June.-12	DGS-1500-20	A1
Runtime: v1.10.005 Boot: 1.00.011	23-Feb.-12	DGS-1500-20	A1
Runtime: v1.10.001 Boot: 1.00.011	12-Jan.-12	DGS-1500-20	A1
Runtime: v1.00.015 Boot: 1.00.010	25-Aug.-11	DGS-1500-20	A1
Runtime: v1.00.013 Boot: 1.00.009	4-July.-11	DGS-1500-20	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 command:

Command	Function
download{firmware_fromTFTP tftp://ip-address/filename cfg_fromTFTP tftp://ip-address/filename}	Download firmware file from the TFTP server to the switch.

When completing firmware upgrade, the following messages will pop up.

```
Device will reboot after firmware upgraded successfully
Image upgraded successfully
```

4. Execute the following command to check the firmware version and switch's information.

Command	Function
show switch	Display the information of current firmware and boot version.

Example:

1. **DGS-1500-20:**
Command: download firmware_fromTFTP tftp://10.90.90.91 DGS-1500-20 A1_2_00_015.hex
Device will reboot after firmware upgraded successfully
Image upgraded successfully
2. **DGS-1500-20:**
Command: show switch
DGS-1500-20> show switch
System name :
System Contact :
System Location :
System up time : 0 days, 1 hrs, 8 min, 36 secs
System Time : 06/15/2012 01:58:42
System hardware version : A1
System firmware version : 2.00.015
System boot version : 1.00.013
System Protocol version : 2.001.004
System serial number : 00SQA15002088
MAC Address : 00-15-00-20-08-88

Upgrade using Web-UI

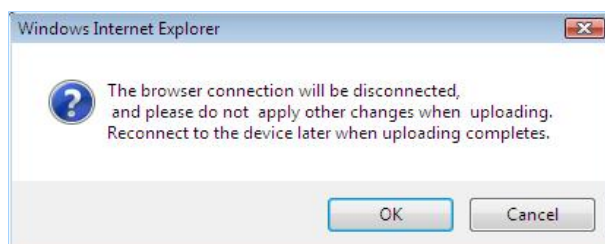
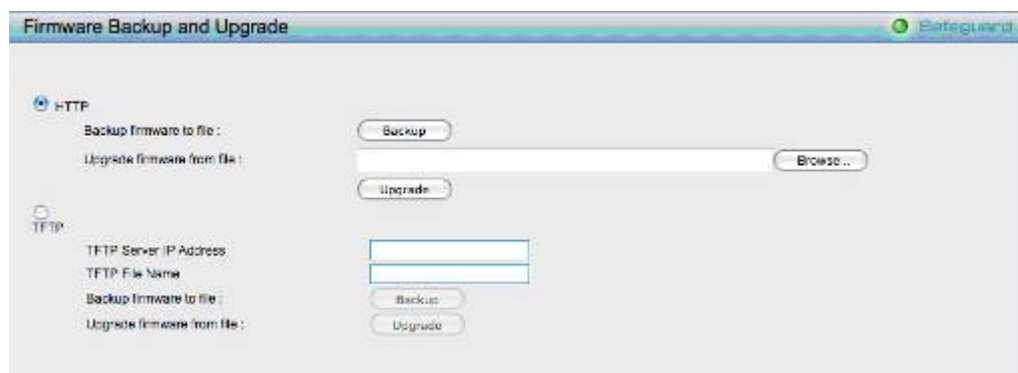
1. Connect a workstation installed with java SE runtime environment to any switch port of the device.
2. Open the web browser from the workstation and enter the IP address of the switch. The

switch's default IP address is 10.90.90.90.

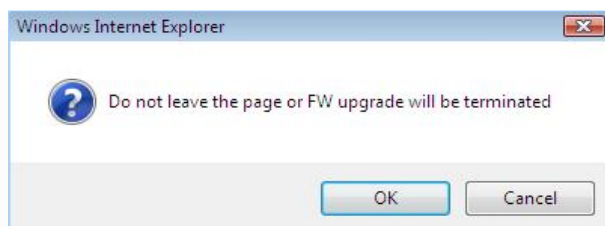
3. Enter administrator's password when prompted. The password is **admin** by default.
4. To update switch's firmware or configuration file, select **Tools > Firmware Backup & Upgrade** from the banner.



5. Two methods can be selected : **HTTP** or **TFTP**



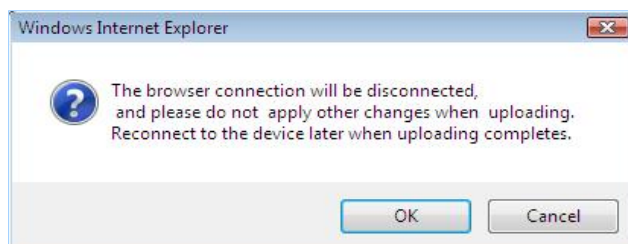
- d. Click **OK** to continue with firmware upgrade



- e. Wait until the "Firmware Upgrade Successful" message pops up and login again after device boots up.



7. Select **TFTP** to upgrade the firmware to or from a remote TFTP server.
 - a. Enter the name of the firmware file located on the TFTP server
 - b. Click **Upgrade** after selecting the firmware file you want to restore
 - c. Click **OK** to continue with firmware upgrade

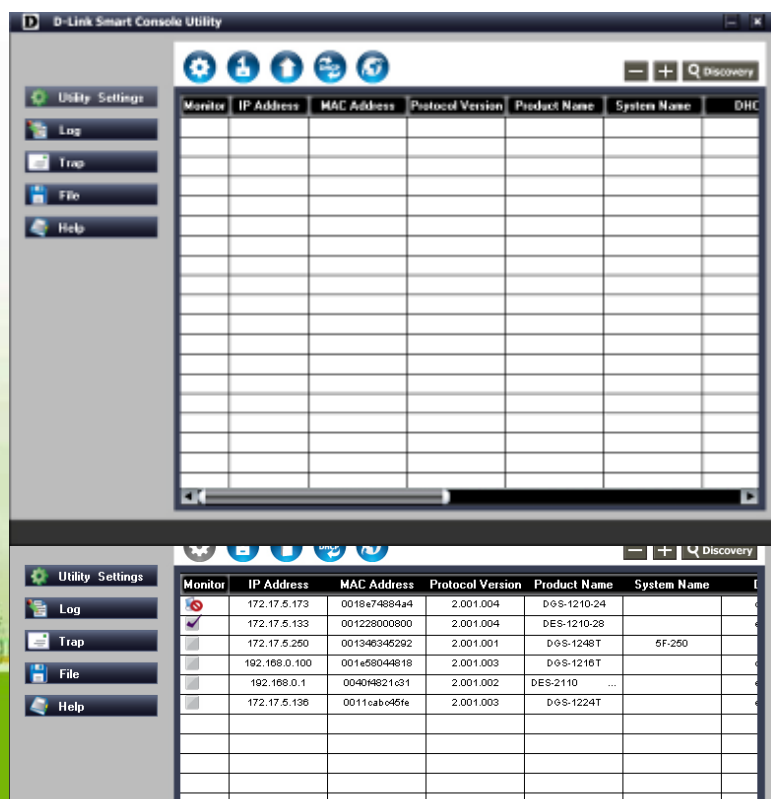


- d. Wait until the firmware upgrade ends and login again after device boots up.



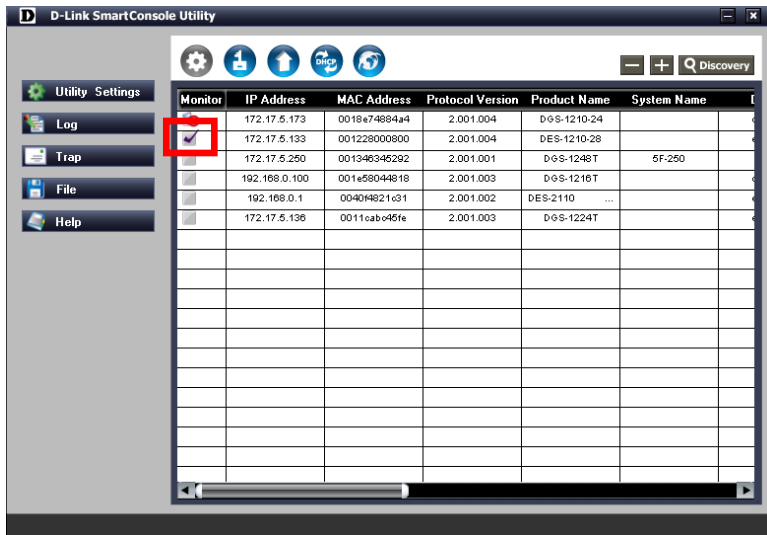
Upgrade using SmartConsole Utility

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

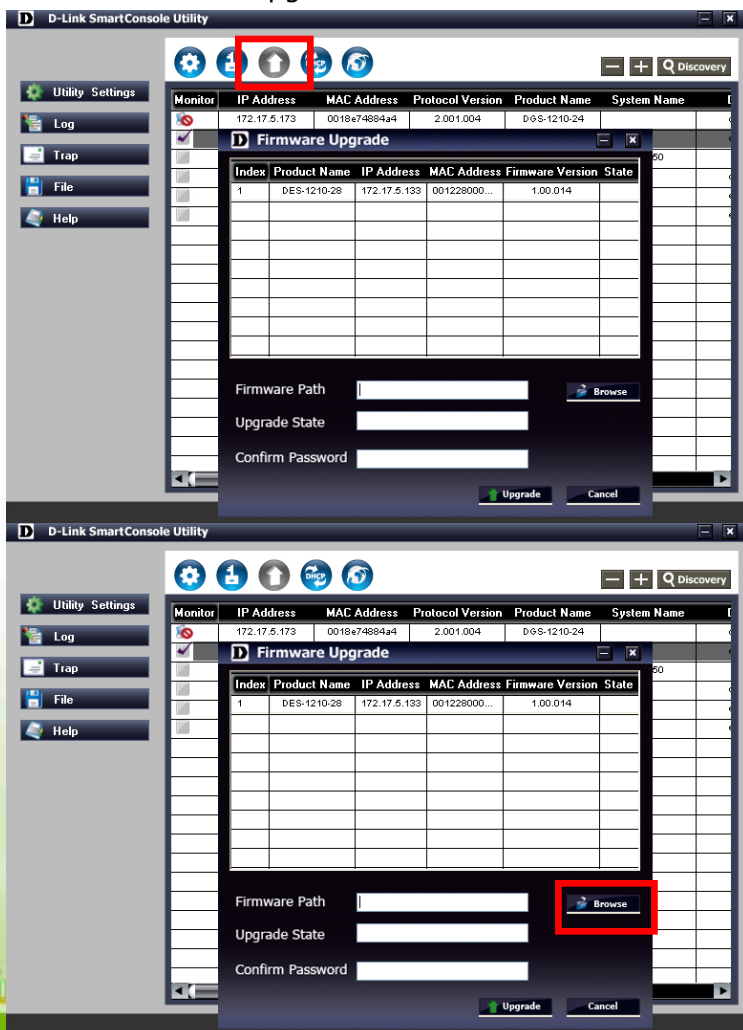




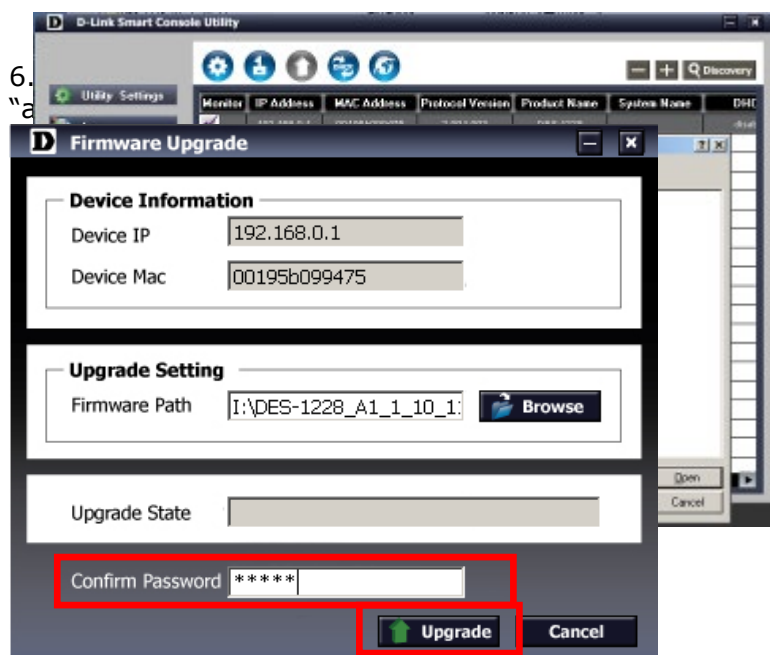
3. Single click the icon of Monitor column to choose the target switch



4. Click Firmware Upgrade button

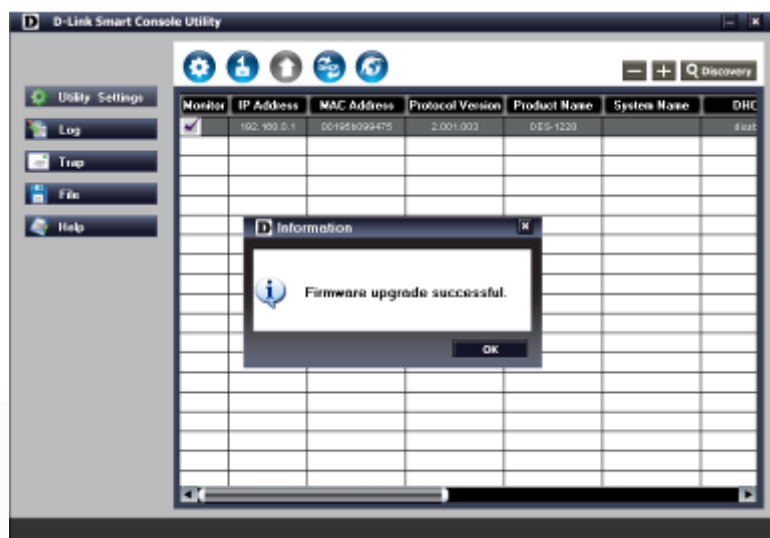


del name_HW ver._FW ver. .hex) on your



ware upgrade. The default password is

7. Once the message popped up, click "OK" button to complete the firmware upgrade



New Features:

Firmware Version	New Features
V2.51.B022	NA

V2.51.B021	NA
V2.51.B019	NA
V2.51.B018	NA
V2.51.B017	NA
V2.51.B016	NA
V2.51.015	NA
V2.51.014	NA
V2.51.B011	NA
V2.51.B010	NA
V2.51.B009	NA
V2.51.B008	NA
V2.51.B007	NA
V2.51.B006	NA
V2.51.005	NA
V2.51.B002	NA
V2.50.B009	1. Add New default MAC (B0C5540 ~ B0C5547) for ASV.

V2.50.008	1. Enhance Zone Defense to 1.07
V2.50.B004	NA
V2.50.003	NA
V2.50.B002	NA
V2.50.B001	1. DDP per port enabled/disabled via Web page. 2. DDP configuration via Web page.
V2.10.B020	NA
V2.10.B019	NA
V2.10.002	NA
V2.00.015	1. Add IPv6 Function include Ipv6 interface, Ipv6 Neighbor, Ipv6 Static Route, Ipv6 SNTP, Ipv6 Traffic Class, Ipv6 Telnet, Ipv6 SSL, Ipv6 Radius Server, Ipv6 ACL, Ipv6 SNMP, Ipv6 Trust Host, Ipv6 DHCP Server Screen and Ipv6 System log. 2. Change LBD and STP enable limitation from per-System to per-port. 3. LBD spec support D-Link LBD 4.04, when enable LBD interface loop to disable. 4. Add STP function to support MSTP Function. 5. Add Forward BPDU function in STP settings page. 6. Add Ipv4/Ipv6 SSH Function. 7. Modify EEE Settings from per-System to per-Port settings. 8. Add ToS Priority Function. 9. Add QoS support TCP/UDP Priority. 10. Add Smart Binding Function. 11. Single IP Management support IPv6 address to connect client Web UI.
V1.10.005	NA
V1.10.001	NA
V1.00.015	NA

V1.00.013

First Release

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 from <http://tsd.dlink.com.tw>. For detailed changes of MIB content, please refer to the modification history in each MIB file.

Firmware Version	MIB File	New Features
V2.51.B022	NA	NA
V2.51.B021	NA	NA
V2.51.B019	NA	NA
V2.51.B018	NA	NA
V2.51.B017	NA	NA
V2.51.B016	NA	NA
V2.51.015	NA	NA
V2.51.014	NA	NA
V2.51.B011	NA	NA
V2.51.B010	NA	NA
V2.51.B009	NA	NA
V2.51.B008	NA	NA
V2.51.B007	NA	NA
V2.51.B006	NA	NA
V2.51.005	NA	NA
V2.51.B002	NA	NA
V2.50.B009	ZoneDefense.mib DGS-1500-20_AX_2_50_002.mib	NA
V2.50.008	ZoneDefense.mib DGS-1500-20_AX_2_50_002.mib	1. Enhance Zone Defense MIB to 1.07 2. Add object "aclL2RulePriority", "aclL2RuleReplacePriority", "aclL3RulePriority", "aclL3RuleReplacePriority", "aclv6L3RulePriority" and "aclv6L3RuleReplacePriority" for ACL.

V2.50.B004	DGS-1500-20_AX_2_50_001.mib	NA
V2.50.003	DGS-1500-20_AX_2_50_001.mib	NA
V2.50.B002	DGS-1500-20_AX_2_00_008.mib	NA
V2.50.B001	DGS-1500-20_AX_2_00_008.mib	NA
V2.10.B020	DGS-1500-20_AX_2_00_008.mib	NA
V2.10.B019	DGS-1500-20_AX_2_00_008.mib	NA
V2.10.002	ZoneDefense.mib DGS-1500-20_AX_2_00_008.mib	NA
V2.00.015	ZoneDefense.mib DGS-1500-20_AX_2_00_008.mib	1. Add IPv6 Function include Ipv6 interface, Ipv6 Neighbor, Ipv6 Static Route, Ipv6 SNMP, Ipv6 Traffic Class, Ipv6 Telnet, Ipv6 SSL, Ipv6 Radius Server, Ipv6 ACL, Ipv6 SNMP, Ipv6 Trust Host, Ipv6 DHCP Server Screen and Ipv6 System log. 2. Change LBD and STP enable limitation from per-System to per-port. 3. LBD spec support D-Link LBD 4.04, when enable LBD interface loop to disable. 4. Add STP function to support MSTP Function. 5. Add Forward BPDU function in STP settings page. 6. Add Ipv4/Ipv6 SSH Function. 7. Modify EEE Settings from per-System to per-Port settings. 8. Add ToS Priority Function. 9. Add QoS support TCP/UDP Priority. 10. Add Smart Binding Function. 11. Support Zone Defense MIB settings to deny all ports ingress IP address. (Only support IPv4 address deny

		settings)
V1.10.005	DGS-1500-20_A1_1_00_008.mib	NA
V1.10.001	DGS-1500-20_AX_1_00_008.mib	NA
V1.00.015	DGS-1500-20_AX_1_00_008.mib	NA
V1.00.013	DGS-1500-20_AX_1_00_008.mib	First Release

Firmware Version	D-View Module File	New Features
V2.51.B022	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B021	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B019	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B018	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B017	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B016	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.015	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.014	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA

V2.51.B011	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B010	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B009	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B008	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B007	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B006	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.005	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.51.B002	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.50.B009	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.50.008	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.50.B004	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.50.003	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.50.B002	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.50.B001	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA

V2.10.B020	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.10.B019	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.10.002	DV_DGS-1500-20_V1.0.0.7_FW_V2.10.002.exe	NA
V2.00.015	DV_DGS-1500-20_V1.0.0.7_FW_V2.00.015.exe	NA
V1.10.005	DV_DGS-1500-20_V1.0.0.7_FW_V1.10.005.exe	NA
V1.10.001	DV_DGS-1500-20_V1.0.0.7_FW_V1.10.001.exe	NA
V1.00.015	DV_DGS-1500-20_V1.0.0.7_FW_V1.00.015.exe	NA
V1.00.013	DV_DGS-1500-20_V1.0.0.7_FW_V1.00.013.exe	First Release

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
V2.51.B022	NA
V2.51.B021	NA
V2.51.B019	NA
V2.51.B018	NA
V2.51.B017	NA
V2.51.B016	NA
V2.51.015	NA

V2.51.B011	NA
V2.51.B010	NA
V2.51.B009	NA
V2.51.B008	NA
V2.51.B007	NA
V2.51.B006	NA
V2.51.005	NA
V2.51.B002	NA
V2.50.B009	NA
V2.50.008	NA
V2.50.B004	NA
V2.50.003	NA
V2.50.B002	NA
V2.50.B001	NA
V2.10.B020	NA
V2.10.B019	NA
V2.10.002	NA
V2.00.015	NA
V1.10.005	NA
V1.10.001	NA
V1.00.015	NA
V1.00.013	First Release

Problem Fixed:

Firmware Version	Problems Fixed
V2.51.B022	1. Issue No: HQ20180328000009 Subject: DGS-1500 issue with CARP[DRU20180328000001-Russia] Description: Device work incorrectly with CARP entries.
V2.51.B021	1. Issue No: HQ20170823000009 DGS-1500 drops mpls ldp packets 2. Remove CLI backdoor

V2.51.B019	1. Fix browser auto save website account and password incorrect issue.
V2.51.B018	1. Increase security with web login. 2. Fix change password with special characters, cannot login issue. 3. WebGUI will login timeout after we enter "Port Statistics".
V2.51.B017	Fix Security Incident Report issue, that include 1. Change the password field in the html file to replace with "check" or other suitable field. 2. To remove the concern, we suggest to run hash on the client side, too. In other words, please change the java script to make sure client will send out new password which is been hashed and send to switch. Then switch need to run hash with its original password and compare these two string are the same. 3. Gamebit value should be hashed. It will help to make sure to randomize gamebit value from user point of view. 4. Make sure the issue of user can download configuration file with any authentication will be fixed.
V2.51.B016	1. Fix DGS-1210-10P the Admin password can be changed by everybody without knowing the Admin password.[DEUR20150813000005-Central Europe].
V2.51.015	1. Fix Multilanguage DE issue.
V2.51.B011	1. [DRU20150114000003-Russia]DGS-1500 issue with IGMP Snooping. 2. Fix DGS-1500 series can not backup firmware when use tftp ipv6 server
V2.51.B010	1.Fix DHCP relay with tag packet issue.When DHCP relay enable but received packet is incoming from vlan without interface,check packet is tagged or not. If yes, untag the packet.BUG ID: Error #9313[DES-1210 transit multicast issue [rostelecom]
V2.51.B009	1. Fix DHCP Local Relay does not work with tagged port.
V2.51.B008	1. Update Boot version to 1.00.017 to fix Hardware version change after upgraded firmware issue [DI20141024000005-Japan].
V2.51.B008	1. [DI20140804000001-Japan]DGS-3120 does not reply to ping if DGS-1500 is rebooted. (Fiber issue) 2. [DGC20140801000004-Taiwan] DGS-1210-28 can't show the specific igmp group.
V2.51.B007	1. OpenSSL before 0.9.8za, which allows man-in-the-middle attack, and consequently hijack sessions or obtain sensitive information. 2. [DI20140804000001-Japan]DGS-3120 does not reply to ping if DGS-1500 is rebooted.
V2.51.B006	1. [DEUR20140612000006-South Europe]Reboot alone after vlan + ip interface configuration. 2. [DRU20140704000004-Russia]DGS-1500 issue with OSPF packets tagging.
V2.51.005	1. [DEUR20140429000003-Eastern Europe] RFC3580 radius attribute mismatch. 2. [DRU20140512000003-Russia] DGS-1500-20 issue with device reboot. 3. Modify STP edge default value to "True". 4. Modify DDP Report Timer default value to "Never"
V2.51.B002	1. [DRU20140326000004-Russia]DGS-1500 issue with ARP Flood. 2. [DEUR20140320000006-Central Europe]DGS-1500-28 the network traffic will slow down and later no more traffic is possible. 3. [DI20140305000005-India]For DGS-1500-28 Not able to create ip interface with subnet mask /30.

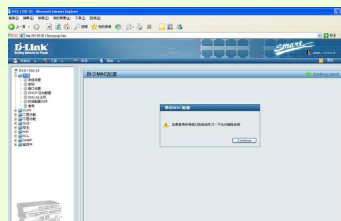
V2.50.B009	1. [DI20140205000006-Japan]Fixed system up time issue. 2. [DRU20140120000004]DES-1210-28 issue with ACL. 3. Modify ASV MAX OUI number to 10.
V2.50.008	1. Enhance DDP to 0.24 2. ACL and QOS page modify. 3. [DRU20131101000002-Russia]Fix telnet issue that DUT with reboot during telnet session. 4. [DI20131031000001-Japan]DGS-1210 does send frames of loopdetect. 5. [DGC20131016000004-Taiwan]DGS-1210-52 with recovery system issue. 6. HQ20130402000005 [DRU20130401000001-Russia]: DGS-1500 series support enhance route.
V2.50.B004	1. HQ20131128000015 [DEUR20131118000008-North Europe] Fixed Time profile could be over night.
V2.50.003	1. Enhance DDP to 0.24 2. ACL and QOS page modify. 3. [DRU20131101000002-Russia]Fix telnet issue that DUT with reboot during telnet session. 4. [DI20131031000001-Japan]DGS-1210 does send frames of loopdetect. 5. [DGC20131016000004-Taiwan]DGS-1210-52 with recovery system issue. 6. HQ20130402000005 [DRU20130401000001-Russia]: DGS-1500 series support enhance route.
V2.50.B002	1. HQ20131128000015 [DEUR20131118000008-North Europe] Fixed Time profile could be over night.
V2.50.B001	NA
V2.10.B020	1. [Support Request] Fix Ping / Login Failure issue in SmartSW series. Note: After confirm with D-LINK Shan, this issue can not find out the correct D-track no. and will keep asking the result for the latest firmware. 2. [DEUR20131008000003-Central Europe] Fixed not able to set STP external cost on Port 9&10 in LAG 3. [DI20130913000003-Japan] Customer has a question about SNMP v1 trap about Enterprise OID and agent-Address. 4. [DI20131017000001-Japan] SNMP trap overlapping. 5. [DI20131023000005-Japan] RSTP switch back will cause network disconnection.
V2.10.B019	1. Fix D-Track [HQ20130723000007][DEUR20130722000012-South Europe] : - Ping failed issue. 2. Fix D-Track [DRU20130812000001-Russia]: - Static router port cannot update into multicast forwarding table in some case.
V2.10.002	1. Fix the bug of JMicron NIC EEE Compatibility test with Marvell Solution. 2. Fix SFP interface compatibility issue. 3. Change EEE default config to disabled. 4. Fix "IEEE802.3az EEE settings" issue at multi-language. 5. Fix "Static MAC" issue at multi-language.
V2.00.015	NA
V1.10.005	1. Download switch configuration without authentication. 2. Routing Table Finder issue. 3. Maximum static route (32 entries) warning message issue. 4. Static Route doesn't work on trunk. 5. Fixed a lot of Simplified Chinese wording error. 6. Fixed Hyperlink issue at the DeviceInfo page. 7. Link issue with DES-1005P.

V1.10.001

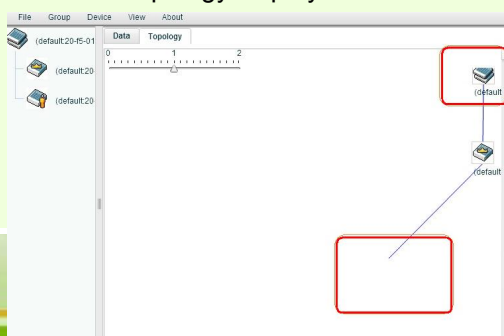
1. Added in additional MAC address range(28107B 000000 ~ 28107B 3FFFFFF) for the ASV function
2. Revised Static Route settings:
 - (1) Support Default Route on All interfaces.
 - (2) Members of all interface VLAN will be added as static route rule member, to fix the host which is in the same VLAN with Gateway can not connect to WAN.
3. Revised Static ARP settings:
 - (1) Add "delete" button on ARP table for user to delete selected ARP entries.
 - (2) Add some information on the ARP table to identify ARP entry (like active/inactive).
 - (3) Support learn Dynamic ARP packets for Route

V1.00.015

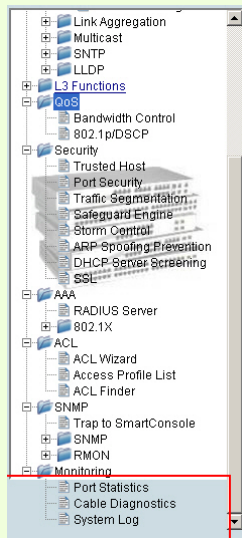
1. User login DUT with interface two, but Web UI show default interface IP.
2. The" 802.1x Authentication failure" system log cannot forward when 802.1 x clients authorized fail.
3. When the ports that already entered "Port Stand-by" status then waked up by ingress packets, then back to "Port Stand-by" status after 10 minutes idle time, DUT CPU always can't respond to ping command.
4. When we create two VLAN IP interfaces then set one of VLAN groups to ASV VLAN then join control PC MAC to ASV OUI, we find the control PC cannot ping (ARP not ICMP) to the DUT after join to ASV dynamic member a while. The DUT ARP Table display IP interface incorrect.
5. When we enable all ports of the DUT port-based Loopback Detection mode then change to VLAN-Based mode, we find the SFP interfaces of the DUT loopback detection function do not work.
6. We find SIM and 802.1X quick configurations page link error in all multi languages besides English.
7. After save config we find wrong page and message in Chinese.



8. Modify default System Time to 01/01/2011.
9. The drop-down fields of Time Profile 1 and 2 always show "None" instead of correct profile name when the profile name is more than 1 character.
10. First create VLAN2 then add port2 to Tag member and change PVID to 2 then add port3 to tag member, we find port2 PVID will change to 1. (We suggest don't change tag port PVID when untag change to tag and keep it by user manual).
11. First change TX Hold Multiplier to 2 then change TX Interval to 32767, then change TX Hold Multiplier to 3 and TX Interval to 120, we find the message "Invalid Message TX Hold Multiplier."
12. We suggest add "clear" button in LLDP Statistics Table.
13. The SIM Topology display error when we move device ICON, please see attach picture.



14. Web UI displays abnormally in Firefox 5.0 under Fedora 9

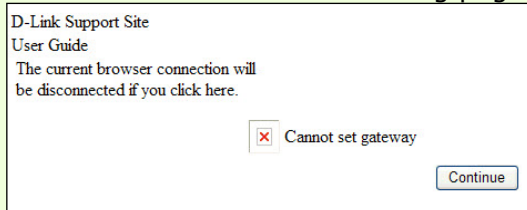


15. In LBD VLAN-based mode, there has no logs about Loop Occurred displayed on the System Log page.

System Log			
Maximum 512 entries.			
Refresh Clear			
ID	Time	Log Description	Severity
1	Jan 5 19:47:59 2009	Port 8 LBD port VID 10 recovered. Loop detection restarted.	info
2	Jan 5 19:48:59 2009	Port 8 LBD port VID 10 recovered. Loop detection restarted.	info
3	Jan 5 19:45:59 2009	Port 8 link up, 1Gbps FULL duplex	info
4	Jan 5 19:45:46 2009	Port 8 link down	info
5	Jan 5 19:45:09 2009	Port 8 LBD port VID 10 recovered. Loop detection restarted.	info

16. The configuration to apply Smart Wizard option "Ignore the wizard next time" will be lost after DUT saving and reboot.

17. If apply DUT's IP address as the gateway in Smart Wizard, the web will redirect to the incorrect warning page.



18. The maximum entity of System Log doesn't match the WebUI description.

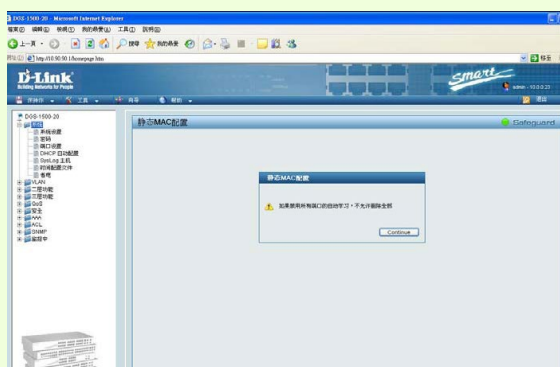
System Log			
Maximum 512 entries.			
ID	Time	Log Description	
491	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
492	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
493	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
494	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
495	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
496	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
497	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
498	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
499	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	
500	Jan 1 15:21:38 2009	Port security violation (Port 2, Vid: 1, MAC: 00-00-03-00-0D-00)	

	19. The behavior that Edge Port of RSTP disconnects and then re-connect to DUT will let DUT to propagate TCN. 20. When DUT receives TCN, the FDB entries of other ports (except the receive port) should flush, but actually not. 21. After save and reboot, the ASV dynamic port member will change to VLAN 1.
V1.00.013	First Release

Known Issues:

Firmware Version	Issues	Workaround
V2.51.B022	None	None
V2.51.B021	None	None
V2.51.B019	None	None
V2.51.B018	None	None
V2.51.B017	None	None
V2.51.B016	None	None
V2.51.015	None	None
V2.51.014	None	None
V2.51.B011	None	None
V2.51.B010	None	None
V2.51.B009	None	None
V2.51.005	None	None
V2.51.B002	None	None
V2.50.B009	None	None
V2.50.008	None	None
V2.50.B002	None	None
V2.50.B001	None	None
V2.10.B020	None	None
V2.10.B019	None	None
V2.10.002	None	None
V2.00.015	None	None
V1.10.005	None	None
V1.10.001	None	None
V1.00.015	None	None
V1.00.013	1. User login DUT with interface two, but Web UI show default interface IP. 2. The" 802.1x Authentication failure" system log cannot forward when 802.1 x clients authorized fail. 3. When the ports that already entered "Port Stand-by" status then waked up by ingress packets, then back to "Port Stand-by" status afetr 10 minutes idle time, DUT CPU always can't respond to ping command.	None

4. When we create two VLAN IP interfaces then set one of VLAN groups to ASV VLAN then join control PC MAC to ASV OUI, we find the control PC cannot ping (ARP not ICMP) to the DUT after join to ASV dynamic member a while. The DUT ARP Table display IP interface incorrect.
5. When we enable all ports of the DUT port-based Loopback Detection mode then change to VLAN-Based mode, we find the SFP interfaces of the DUT loopback detection function do not work.
6. We find SIM and 802.1X quick configurations page link error in all multi languages besides English.
7. After save config we find wrong page and message in Chinese.



8. We uplink two DUT and set one fiber port to force mode, we find still link successful
9. We find uplink two DUT the port link status will link up-->link down--> link up when power saving is enable.
10. We find Fiber port LED glitter frequency not stable.
11. When DUT enter or leave "LED Shut-off" status, PC's NIC will link down then link up.
12. MAC addresses of DUT SFP ports in FDB will be cleared when new link is established in DUT SFP ports. This issue also exists in copper ports randomly.
13. When two ports transmit packets to the same destination port with the same queue, the received rate is not stable.
14. We find storm control rate is not accurate, tolerance about 76%.
15. Sometimes when we test interface cable diagnostics function, the interface will shutdown then link up again.

Related Documentation:

- DGS-1500-20 Series User Manual
- DGS-1500-20 Series Getting Started Guide