Firmware Version:	4.10.004
Boot Code Version:	1.00.016
MIB Version:	4.10.002
D-View Module Version:	4.0.0.5
Published:	Dec. 11, 2015

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: v4.10.004 Boot: 1.00.016	15- Dec.-15	DGS-1210-20/28/52/28P/10/52P/10P/52MP	C1
Runtime: v4.00.J066 Boot: 1.00.005	20-Apr.-15	DGS-1210-20/28/52/28P/10/52P/10P/52MP	C1 (for DJP only)
Runtime: v4.00.064 Boot: 1.00.016	02- Feb.-15	DGS-1210-20/28/52/28P/10/52P/10P/52MP	C1
Runtime: v4.00.057 Boot: 1.00.016	06- Oct.-14	DGS-1210-20/28/52/28P/10/52P DGS-1210-10P/52MP(new)	C1
Runtime: v4.00.055 Boot: 1.00.016	04-Sep.-14	DGS-1210-20/28/52/28P DGS-1210-10/52P (new)	C1
Runtime: v4.00.012 Boot: 1.00.005	08- Aug.-13	DGS-1210-20/28/52/28P	C1 (First release)

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-1210-10:
   Command: download firmware_fromTFTP tftp://10.90.90.91
   DGS-1210-52P-C1-4-00-055.hex
   Device will reboot after firmware upgraded successfully
   Image upgraded successfully

2. DGS-1210-10:
   Command: show switch
   DGS-1210-52P> show switch
   System name                    :
   System Contact                 :
   System Location                :
   System up time                 : 0 days, 0 hrs, 2 min, 31 secs
   System Time                    : 01/01/2014 00:02:19
   System hardware version        : C1
   System firmware version        : 4.00.055
   System boot version            : 1.00.016
   System serial number           : QBDES12105200
   MAC Address                    : 9C-D6-43-AA-58-77
```

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**
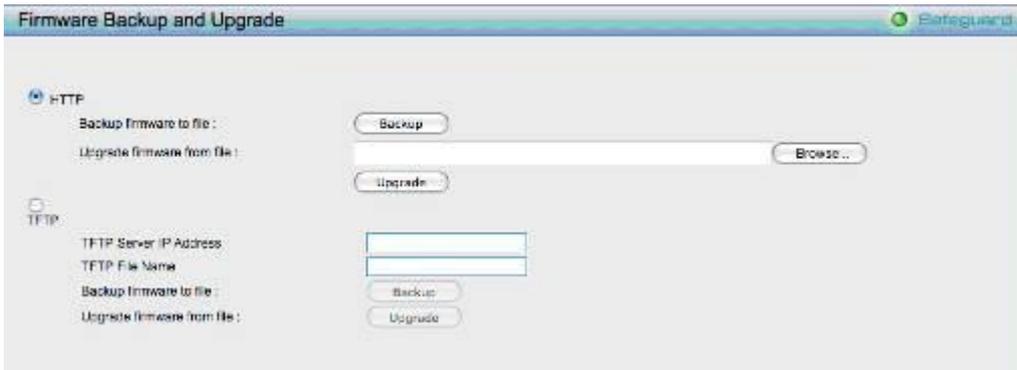
a. Click **Browse** to browse your inventories for a saved firmware file
b. Click **Upgrade** after selecting the firmware file you want to restore
c. Click **OK** to continue with firmware upgrade

d. Click **OK** to continue with firmware upgrade
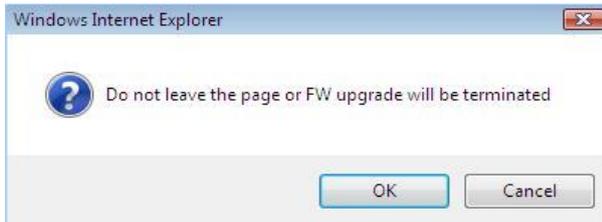
e. Wait until the "Firmware Upgrade Successful" message pops up and login again after device boots up.

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
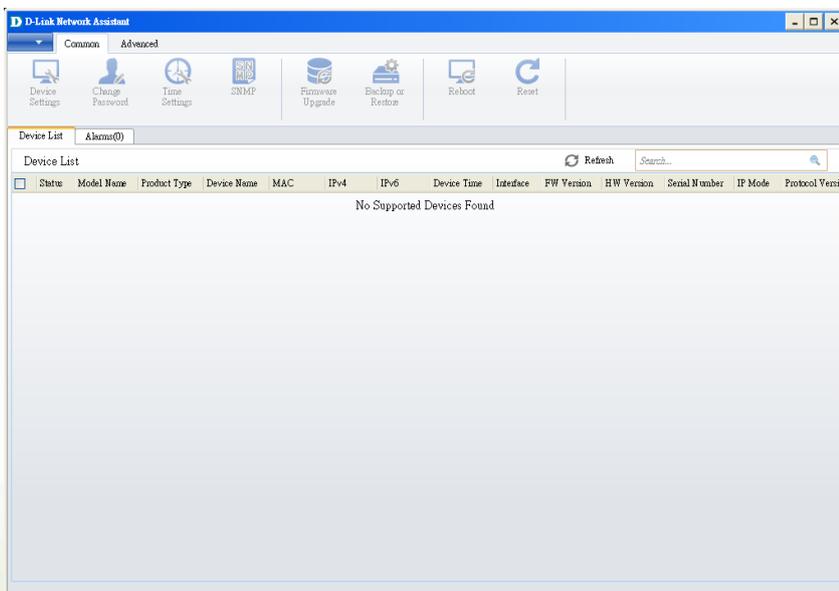c. Click **OK** to continue with firmware upgrade

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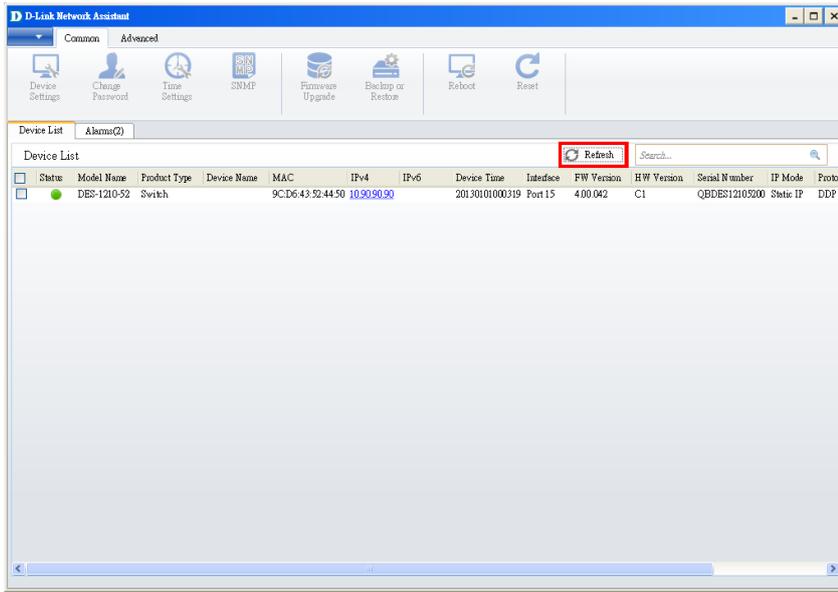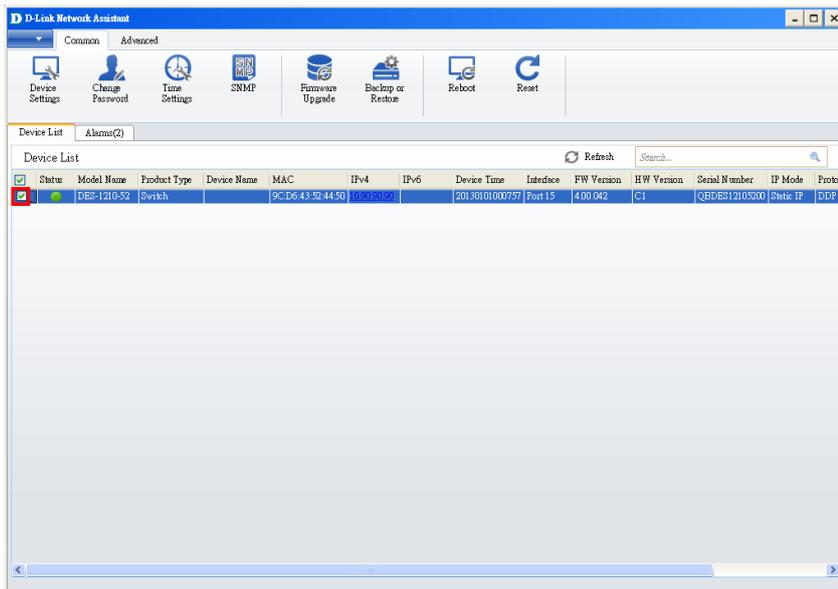

Upgrade using D-Link Network Assistant

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

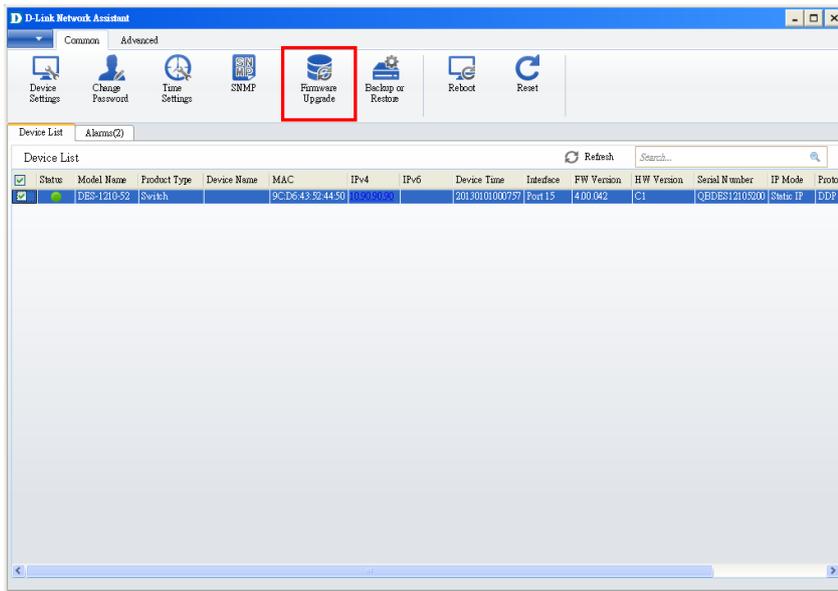2. Execute D-Link Network Assistant

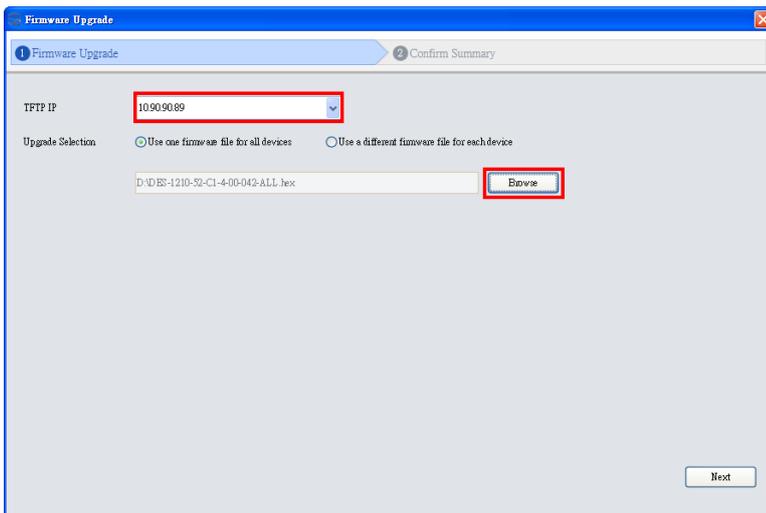3. Click Refresh button to search target switch

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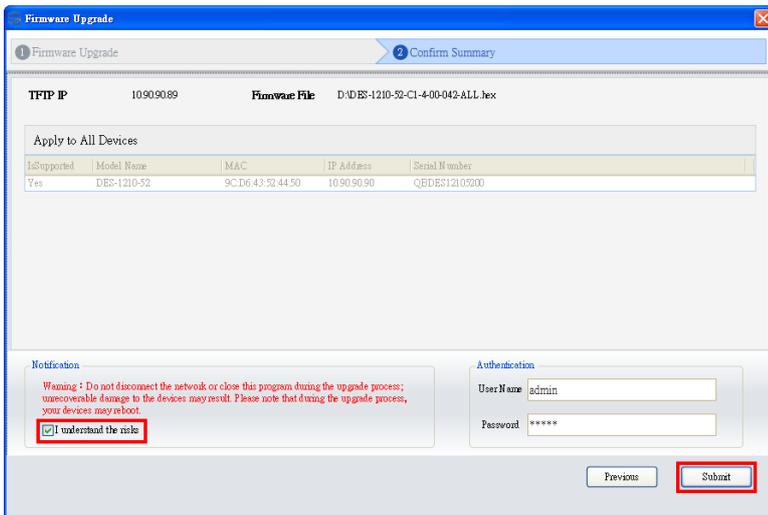
8. Once the message changed to success, click "Close" button to complete and exit the firmware upgrade
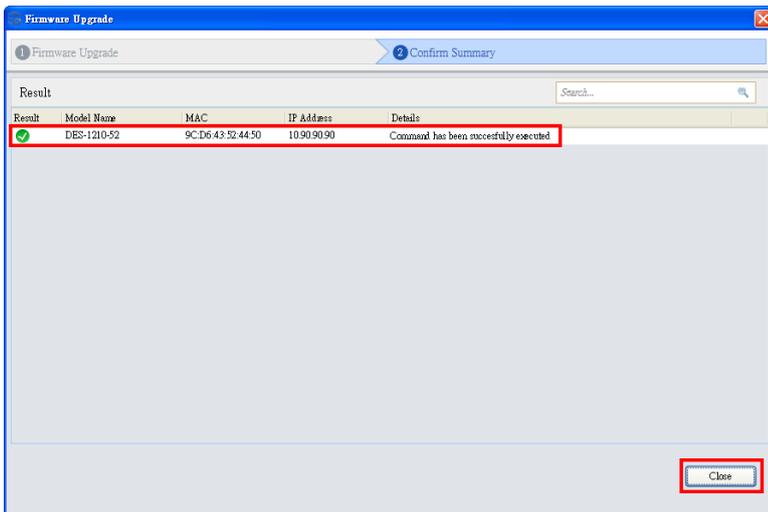
New Features:

Firmware Version	New Features
V4.10.002	1.Support Auto Downgrade on Port Setting [DEUR20151001000012] 2.Support Legacy PD mode option on Web GUI
V4.00.J066	N/A
V4.00.064	N/A
V4.00.057	First Release

V4.00.055	First Release
V4.00.012	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
V4.10.002	DGS-1210-xx-CX-4-10-002.mib	1. Add DHCPRetryTimes object. 2. Add auto downgrade [DEUR20151001000012] 3. Modify cableDiagPairStatus, doSCtrlDisplayState object. 4. Add poePortLegacyPDDetect object 5. Add poePortDelayPowerDetect object for 59111 IOT issue with HIKVision Camera on DGS-1210-28P
V4.00. J066	DGS-1210-xx-CX-4_00_008.mib	N/A
V4.00.064	DGS-1210-xx-CX-4_00_008.mib	N/A
V4.00.057	DGS-1210-xx-CX-4_00_008.mib	N/A
V4.00.055	DGS-1210-xx-CX-4_00_008.mib	N/A
V4.00.012	DGS-1210-xx-CX-4_00_008.mib	First Release

Firmware Version	D-View Module File	New Features
V4.10.002	DV_DGS-1210-10 C1_4.0.0.6_setup.exe	1. Update the Digital Signature
V4.00.J066	DV_DGS-1210-xx C1_4.0.0.4_setup.exe	N/A
V4.00.064	DV_DGS-1210-xx C1_4.0.0.4_setup.exe	N/A

V4.00.057	DV_DGS-1210-52MP C1_4.0.0.4_setup.exe	N/A
V4.00.055	DV_DGS-1210-10/10P/52P C1_4.0.0.4_setup.exe	N/A
V4.00.025	DV_DGS-1210-52 C1_4.0.0.4_setup.exe	N/A
V4.00.012	DV_DGS-1210-20/28/25/28P C1_4.0.0.3_setup.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
V4.10.002	LLDP/LLDP-MED default disabled
V4.00.J066	N/A
V4.00.064	N/A
V4.00.057	N/A
V4.00.055	N/A
V4.00.012	First Release

Problem Fixed:

Firmware Version	Problems Fixed
V4.10.002	1. EEE default is changed from enabled to disabled.

2. Fix security issue on HTML page

3. [DBG15100112] cross-chip issue for unicast traffic. (52 port model only)

4. [DEUR20151120000003-Eastern Europe] Fixed that Port mirror does not mirror outgoing traffic.

5. Fixed the issue that user can download configuration file with any authentication.

6. Fixed the issue that configuration backup button doesn't work.

7. [DEUR20150529000006] Fixed VoiceVLAN bug (DGS-1210 series only)

8. [DI20151015000004-Korea] Fixed Samsung SENS RC420 cannot ping correctly when EEE enabled.

9. [DEUR20151012000003] Change external PHY as master preferred mode.

10. [DGC20151019000003-China] Fixed the problem when IEEE802.3az EEE enabled, Fast Ethernet connection failed.

11. MAC address ACL will be allowed to configure Multicast and Broadcast address.

12. Modified wrong STP cost on LACP links [DRU20150907000006-Russia]

13. Fixed the reboot issue. When users open http://10.90.90.90/config.bin or http://10.90.90.90/config.cfg, switch reboots. [DRU20150907000005-Russia].

14. Fixed one bug on ACL protocol type setting issue. If user doesn't choose Protocol-Type, switch shows the protocol_id 256. [DGC20150921000002-Taiwan]

15. Adding the configurable ACL retry time [DUSA20150721000002]

16. Fixed the problem on to establish LACP Negotiation with Windows Server 2012R2 [DEUR20150819000004-UKI]

17. Modified blat attack DoS type setting. The original blat attack is to block TCP/UDP source port number equal to TCP/UDP destination port number. The new update is to block TCP source port number equal to TCP destination port number. [DRU20150729000002]

18. Adding port configuration of VLAN on Web GUI. [DRU20150903000003]

19. Fixed one bug on DHCP programing code error. [DUSA20150820000002]

20. Fixed the DHCP option 12 bug. [DUSA20150707000001-USA]

21. Fixed the filter unregistered multicast feature doesn't work issue.

22. Fixed one bug. The admin password can be changed by everybody without knowing the Admin password. [DEUR20150813000005-Central Europe]

23. For PoE models, changing 802.3at design spec. as 2-Event Physical Layer classification plus data link layer by default.

24. Adding workaround on OpenSSL issue: CVE-2015-1789 (OpenSSL before 0.9.8zg)
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1789

25. Fixed one bug on MAC ACL setting. Users can't deny more than 2 mac address

	by using ACL function. [DGC20150626000004-Taiwan] 26. Fixed the wrong behavior when using VLAN and LBD at the same time. [DEUR20150722000006-Central Europe] 27. Fixed the problem that IGMP Leave is sent with wrong Source IP[DEUR20150420000001-Eastern Europe]
V4.00.J066	This firmware is to disable EEE by default.
V4.00.064	This firmware is to emend German Web GUI error wordings.
V4.00.057	
V4.00.055	
V4.00.012	First Release

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues	Workaround
V4.00.012	N/A	N/A
V4.00.J066	N/A	N/A
V4.00.064	N/A	N/A
V4.00.057	N/A	N/A
V4.00.055	1. After DUT warm/cold start, SNMP host will only receive cold start trap and link up trap. [DBG14100240] 2. Web UI will not pop-out error message when assign incorrect ACL IPv4 address(Ex:256.255.255.255).[DBG14100248] 3. Use OID (1.3.6.1.4.1.171.10.76.33.1.9.3.1.2) to get static mac address via SNMP will return wrong MAC value.[DBG14100164] 4. When Loopback Detection is disabled, LACP does not work.	Will fixed in future version (V4.10)
	1. The DUT Voice VLAN dynamic untag member does not follow Voice VLAN ID to forward fit OUI packets.Please refer to attach file, Voice VLAN ID is	

3, the fit OUI packets still use VID2 to forward packets not VID3.

2. The DUT Unknow multicast filter enable will cause IPv6 control packets (NS, RS..) be drop by DUT that does not fit D-Link request.

3. "The DUT DHCP Server screen cannot drop incorrect DHCPv6 server packets (not fit white list IPv6 address), the DUT still can get IPv6 address from incorrect DHCPv6 server.

4. The DUT LLDP Management IPv4 Address will be auto deleted after control PC topology change to another interface of the DUT.

5. The DUT LLDP Management IPv4 Address will be auto deleted after set IPv6 management address type via IPv4 address.

6. The DUT SmartBinding black list just can display one entry (IPv4 or IPv6) when this black entry exist IPv4 and IPv6 address.

7. "The DUT SmartBinding Auto Scan binding entry result IPv4 still keep entry after binding entry finish, that different with IPv6.

8. When delete IPv6 trust host, the DUT does not pop-up warning message, but IPv4 trust host support it.

9. "The DUT Static MAC auto learning disable interface still can forward packets to other interface even does not create static MAC. (via ASV default OUI MAC address)After confirm with D-Link Shan, he agree this behavior when forward fit OUI packets to disable auto learning interface at currect state, but still need note to D-Lab Bug System and test report. "

10. "The DUT Voice VLAN Voice device already be update by other auto detect interface, but the VLAN settings still keep before member.
    Test Step:
    1. Create VLAN ID 4000.
    2. Enable Voice VLAN VID 4000.
    3. enable all ports auto detect funciton of Voice VLAN.
    4. Use LLDP packets forward fit Voice VLAN ID info to port24.
    5. Port24 create dynamic member to Voice VLAN.
    6. Use the same LLDP forward fit Voice VLAN ID info to Port28.
    7. Voice VLAN device list info already be update, but Voice VLAN still keep port24

and Port28 dynamic member."

11. Sometimes the DUT STP P2P Function fast change port state does not valid after uplug and plug interface.

12. Follow D-Link test plan, the DUT default settings ping respond need to <= 1 ms, but our DUT cannot fit this request.

13. When change DUT IP settings from Static to BOOTP, the DUT always forward 2 BOOTP request at the same times. The DUT just forward one BOOTP reqest after save config then reboot.

14. "The DUT VLAN Based Loopback detection will cause DUT cannot respond when uplink loop topology.
    Test Step:
       1. Create VLAN ID 256.
       2. Control PC connect to 256 VLAN member.
       3. Enable LBD VLAN mode support VID 1~255 and enable all ports LBD function.
       4. Use port1 (include VID 1~255) uplink to loop topology.
       5. The DUT no respond, we must remove loop topology, the DUT just can reply normally."

15. "The DUT LBD cannot block all ports loop interface after uplink all ports loop after about 10 mins. Port1 connect to port2, port3 connect to port4.... Port23 connect to control PC, Port24 connect to DHCPv4/v6 server.

    The DUT will loop after about 10 mins, the DUT console interface will display error message and loop packets is ICMPv6 (RA) Multicast packets."Franny(2013/07/31) : The number of supported LBD VLAN depends on hardware STG table entries and . If table is full, the switch will not handle the additional loopback VLANs.   For DGS-1210-28, LDB will use 8 STG.

    Therefor, the issue belongs to H/W limitation.

16. "The DUT Auto Sureillance VLAN default OUI does not fit D-Link ASV Spec 1.3.
    D-Link Surveillance Device range should support 28-10-7B-00-00-00 ~ 28-10-7B-2F-FF-FF, but test result 28-10-7B-30-00-00 still can join to dynamic member."

17. The DUT exist Head of Line blocking issue via Jumbo Frame packets.

18. The DUT Mirror Function Target Port always get packets with Tag info from Source port TX even all

ports belong to Untag and forward Untag packets to test.
(PS: Mirror RX funciton does not exist this issue)

19. The DUT Voice VLAN and ASV dynamic member ingress rule still follow original VLAN member rule not Voice or ASV VLAN.

Related Documentation:

- DGS-1210-10 Series User Manual
- DGS-1210-10 Series Getting Started Guide