Firmware Version: 4.00.064
Boot Code Version: 1.00.005
MIB Version: 4.00.008
D-View Module Version: 4.0.0.13
Published: Feb. 02, 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: v4.00.064 Boot: 1.00.005	02-Feb.-15	DGS-1210-28	C1
Runtime: v4.00.063 Boot: 1.00.005	29-Jan.-15	DGS-1210-28	C1
Runtime: v4.00.062 Boot: 1.00.005	22-Jan.-15	DGS-1210-28	C1
Runtime: v4.00.060 Boot: 1.00.005	22-Jan.-15	DGS-1210-28	C1
Runtime: v4.00.B055 Boot: 1.00.005	04-Sep.-14	DGS-1210-28	C1
Runtime: v4.00.B053 Boot: 1.00.005	13-Aug.-19	DGS-1210-28	C1
Runtime: v4.00.B052 Boot: 1.00.005	13-Aug.-14	DGS-1210-28	C1
Runtime: v4.00.B046 Boot: 1.00.005	08-May.-14	DGS-1210-28	C1
Runtime: v4.00.B045 Boot: 1.00.005	08-May.-14	DGS-1210-28	C1
Runtime: v4.00.B039 Boot: 1.00.005	06-Feb.-14	DGS-1210-28	C1
Runtime: v4.00.012 Boot: 1.00.005	08- Aug.-13	DGS-1210-28	C1

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-1210-28:**
   ```
   Command: download firmware_fromTFTP tftp://10.90.90.91
   DGS-1210-28-C1-4-00-012hex
   Device will reboot after firmware upgraded successfully
   Image upgraded successfully
   ```

2. **DGS-1210-28:**
   ```
   Command: show switch
   DGS-1210-28> show switch
   System name                    :
   System Contact                 :
   System Location                :
   System up time                 : 0 days, 0 hrs, 36 min, 56 secs
   System Time                    : 01/01/2013 01:01:55
   System hardware version        : C1
   System firmware version        : 4.00.012
   System boot version            : 1.00.005
   System serial number           : 1MB1733K0000A
   MAC Address                    : 00-87-87-AB-88-77
   ```

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.
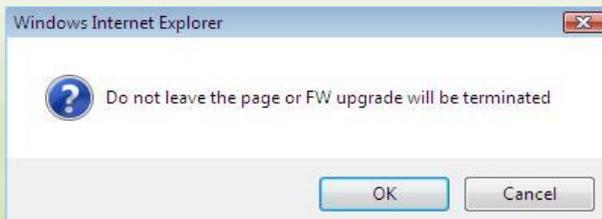

5. Two methods can be selected : **HTTP** or **TFTP**
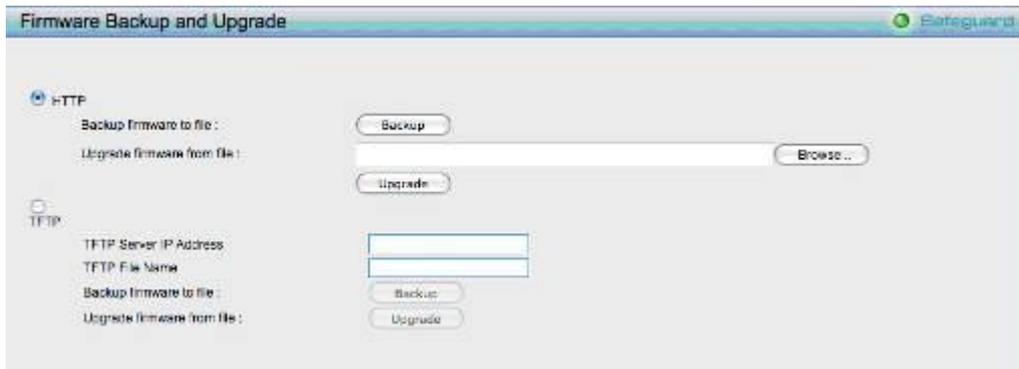
6. Select **HTTP** to upgrade the firmware to or from your local drive of PC.
   a. Click **Browse** to browse your inventories for a saved firmware file
   b. Click **Upgrade** after selecting the firmware file you want to restore
   c. Click **OK** to continue with firmware upgrade

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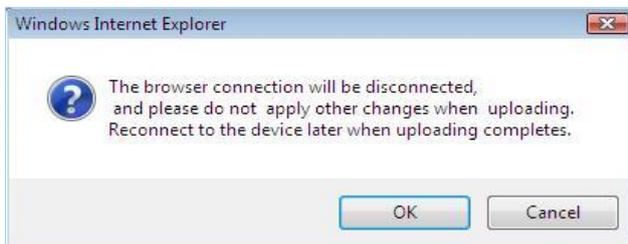
    d. Wait until the firmware upgrade ends and login again after device boots up.
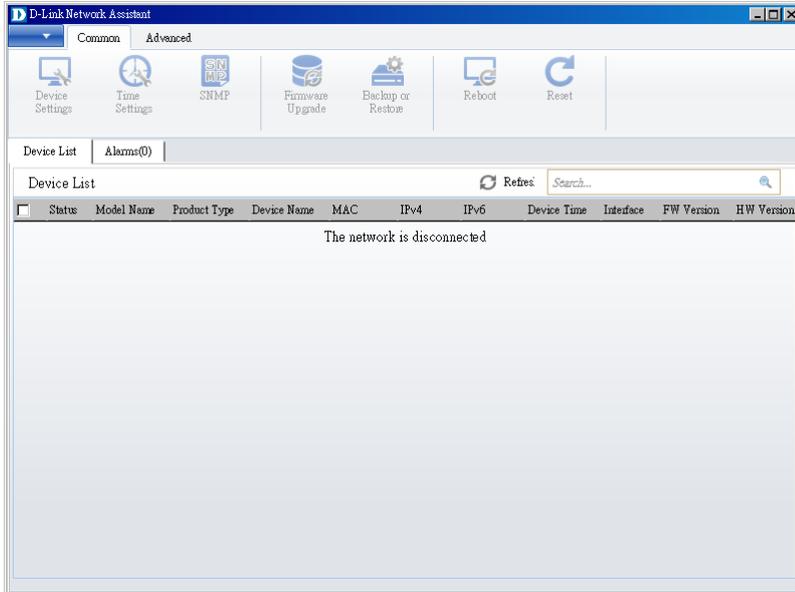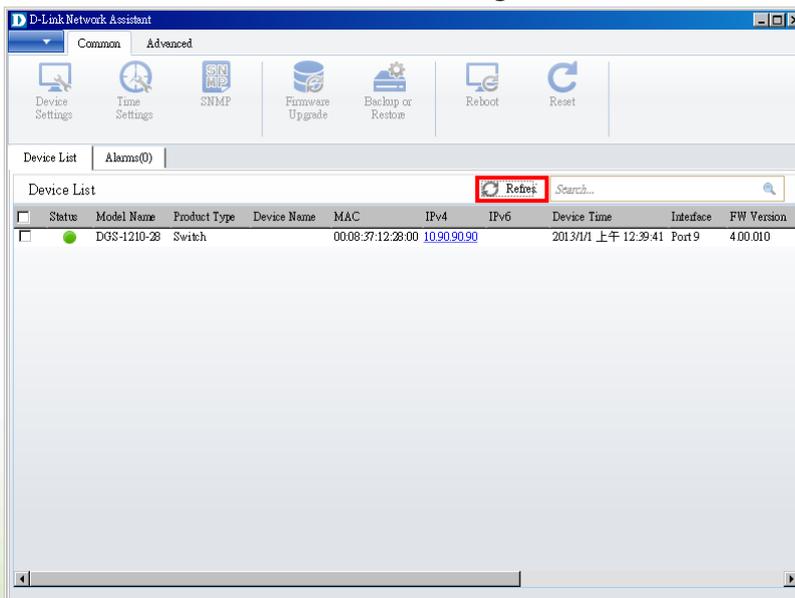

Upgrade using D-Link Network Assistant
1. Connect a workstation installed with java SE runtime environment to any switch port of the
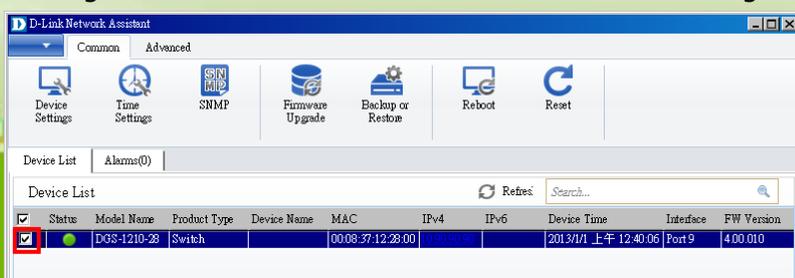
device

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.
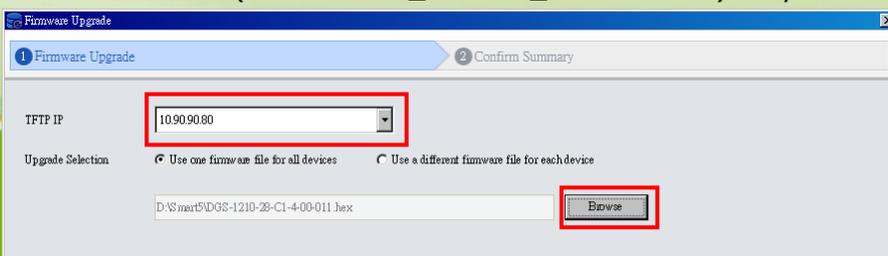
7. Click the checkbox and click "Submit" button to start firmware upgrade.
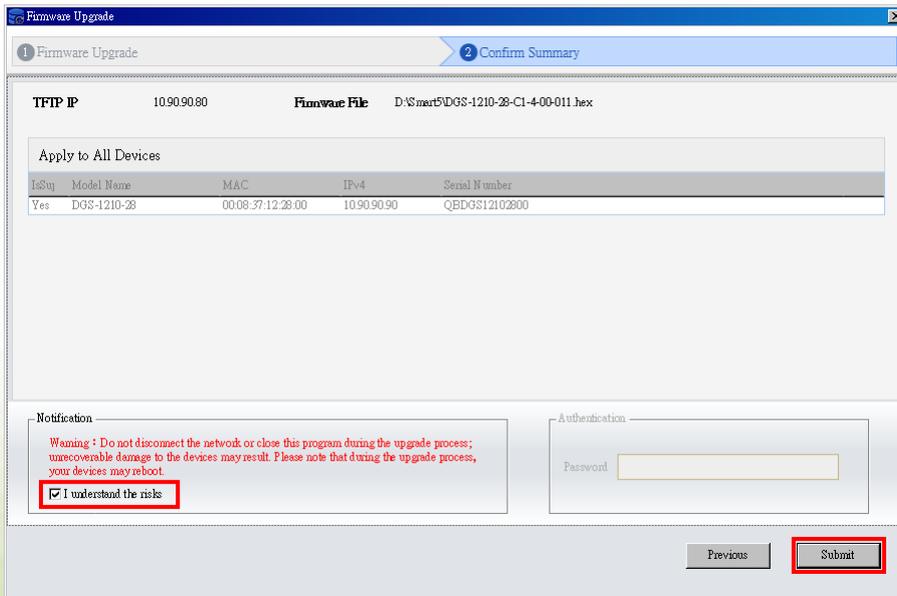
8. Once the message changed to success, click "Close" button to complete and exit the firmware

upgrade

New Features:

Firmware Version	New Features
V4.00.064	N/A
V4.00.063	N/A
V4.00.062	N/A
V4.00.060	N/A
V4.00.B055	N/A
V4.00.B053	N/A

V4.00.B052	N/A
V4.00.B046	N/A
V4.00.B045	N/A
V4.00.B039	N/A
V4.00.012	First Release

Changes of MIB & D-View Module:

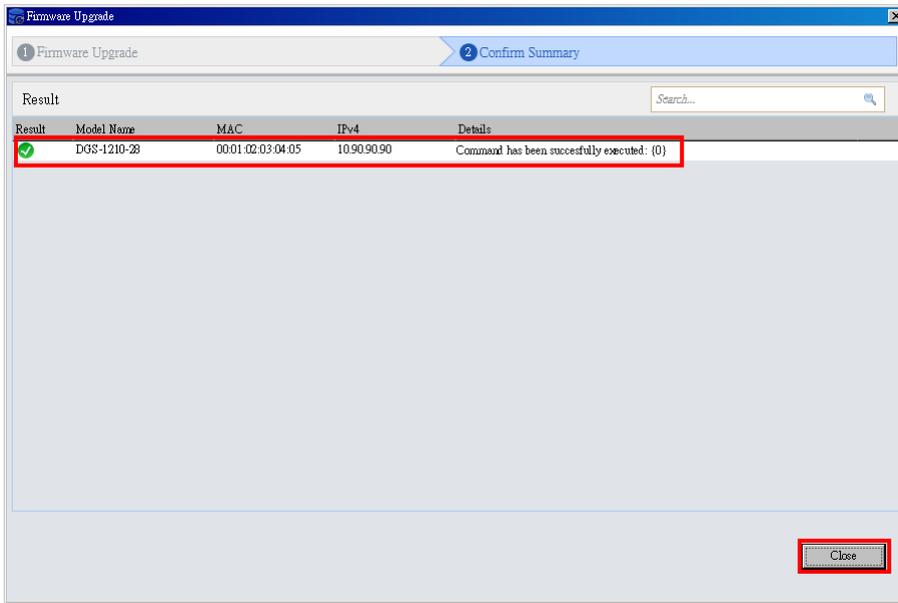The new features of MIB file are also included in the corresponding D-View module. Please download the D-View module from http://tsd.dlink.com.tw. For detailed changes of MIB content, please refer to the modification history in each MIB file.

Firmware Version	MIB File	New Features
V4.00.064	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.063	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.062	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.060	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.B055	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.B053	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.B052	DGS-1210-28-CX-4_00_008.mib	N/A

V4.00.B046	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.B045	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.B039	DGS-1210-28-CX-4_00_008.mib	N/A
V4.00.012	DGS-1210-28-CX-4_00_008.mib	First Release

Firmware Version	D-View Module File	New Features
V4.00.064	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.063	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.062	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.060	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.B055	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.B053	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.B052	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.B046	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.B045	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.B039	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.exe	N/A
V4.00.012	DV_DGS-1210-28_V4.0.0.13_FW_v4.00.012.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
V4.00.064	N/A
V4.00.062	N/A
V4.00.061	N/A
V4.00.060	N/A
V4.00.B055	N/A
V4.00.B053	N/A
V4.00.B052	N/A
V4.00.B046	N/A
V4.00.B045	N/A
V4.00.B039	N/A
V4.00.012	First Release

Problem Fixed:

Firmware Version	Problems Fixed
V4.00.064	1. Fix IPv6 TFTP Fw backup fail..
V4.00.063	1. Fix config backup page at DE language issue.
V4.00.062	1. Fix Multilanguage DE issue.
V4.00.060	1. Fix Multilanguage DE issue.
V4.00.B055	1. Fix incorrect model on SSL certificate.
V4.00.B053	1. [DGC20140801000004-Taiwan] DGS-1210-28 can't show the specific igmp group.
V4.00.B052	1. OpenSSL before 0.9.8za, which allows man-in-the-middle attack, and consequently hijack sessions or obtain sensitive information.

V4.00.B046	1. [DUSA20140530000002-Canada] DGS 1210-28P will not forward LLDP multicast mac address.
V4.00.B045	1. STP edge default value must change to "True".
V4.00.B039	1. Add New default MAC (B0C5540 ~ B0C5547) for ASV. 2. [DBG13120389] There are some packet loss when sends IPV6_CTRL1.str and IPV6_CTRL2.str.
V4.00.012	First Release

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues	Workaround
V4.00.012	N/A	None
V4.00.012	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. D-Link: This issue can note limitation. 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. D-Link: Note can list this issue to be known issue. 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. D-Link: keep this issue and does not need to modify in this stage." 4. The DUT LLDP Management IPv4 Address will be auto deleted after control PC topology change to another interface of the DUT. D-Link: Note Fix next version (2013/11). 5. The DUT LLDP Management IPv4 Address will be auto deleted after set IPv6 management address type via IPv4 address. D-Link: Agree next version (2013/11) to fix this issue. 6. The DUT SmartBinding black list just can display one entry (IPv4 or IPv6) when this black entry exist IPv4 and IPv6 address. D-Link: Does not need to modify. 7. "The DUT SmartBinding Auto Scan binding entry result IPv4 still keep entry after binding entry finish, that different with IPv6. D-Link: Fix in next version (2013/11), and modify ""Bound"" wording to ""Yes""."	V4.00.012

Cameo: Modified "Bound" wording to "Yes" in ver.4.00.010

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. "

   Cameo: Won't fix. (Maximum support 156 VLAN Groups)

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."

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.

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.

Franny(2013/07/31) : The issue belongs to H/W limitation.

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)

Franny(2013/07/31) : The issue belongs to H/W limitation.

19. The DUT Voice VLAN and ASV dynamic member

ingress rule still follow original VLAN member rule not Voice or ASV VLAN.

Franny: We recommed use IFP ("Redirect port = voice VLAN member" + "G_L3SW_CHANGE_L2_FIELDS = 3'd1") + Add Deivce MAC in FDB to confirm if the solution can solve the issue or not.

Therefor, we are waiting for Cameo reply

Related Documentation:

- DGS-1210-28 Series User Manual
- DGS-1210-28 Series Getting Started Guide