Firmware Version: v 3.10.012
Prom Code Version: v 2.00.003
Published: Jan. 21, 2014

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 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 firmware by CLI (serial port) 3
Upgrade firmware by Web-UI 4
DLMS Instructions: 6
DLMS License Activation by CLI 6
DLMS License Activation by Web-UI 7
New Features: 8
Changes of MIB & D-View Module: 10
Changes of Command Line Interface: 12
Problem Fixed: 14
Known Issues: 20
Related Documentation: 21

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
Runtime: v3.10.012 PROM: v2.00.003	21-Jan-14	DGS-3120-24TC	A1, A2 (not compatible to B1)
		DGS-3120-24SC	A1, A2 (not compatible to B1)
		DGS-3120-24SC-DC	A1, A2 (not compatible to B1)
		DGS-3120-48TC	A1, A2 (not compatible to B1)
		DGS-3120-24PC	A1, A2 (not compatible to B1)
		DGS-3120-48PC	A1, A2 (not compatible to B1)
Runtime: v3.00.522 PROM: v2.00.003	18-Mar-13	DGS-3120-24TC	B1 (not compatible with A1/A2)
		DGS-3120-24SC	B1 (not compatible with A1/A2)
		DGS-3120-24SC-DC	B1 (not compatible with A1/A2)
		DGS-3120-48TC	B1 (not compatible with A1/A2)
		DGS-3120-24PC	B1 (not compatible with A1/A2)
		DGS-3120-48PC	B1 (not compatible with A1/A2)
Runtime: v3.00.022 PROM: v2.00.003	4-Feb-13	DGS-3120-24TC	A1, A2
		DGS-3120-24SC	A1, A2
		DGS-3120-24SC-DC	A1, A2
		DGS-3120-48TC	A1, A2
		DGS-3120-24PC	A1, A2
		DGS-3120-48PC	A1, A2
Runtime: v2.50.015 PROM: v2.00.003	6-Apr-12	DGS-3120-24TC	A1, A2
		DGS-3120-24SC	A1, A2
		DGS-3120-24SC-DC	A1, A2
		DGS-3120-48TC	A1, A2
		DGS-3120-24PC	A1, A2
		DGS-3120-48PC	A1, A2
Runtime: v2.00.010 PROM: v2.00.003	20-Jun-11	DGS-3120-24TC	A1, A2
		DGS-3120-24SC	A1, A2
		DGS-3120-24SC-DC	A1, A2
		DGS-3120-48TC	A1, A2
		DGS-3120-24PC	A1, A2
		DGS-3120-48PC	A1, A2
Runtime: v1.02.013 PROM: v1.00.010	20-Jan-11	DGS-3120-24TC	A1
		DGS-3120-24SC	A1
		DGS-3120-24SC-DC	A1
		DGS-3120-48TC	A1
		DGS-3120-24PC	A1
		DGS-3120-48PC	A1
Runtime: v1.01.027 PROM: v1.00.009	31-Dec-10	DGS-3120-24TC	A1
		DGS-3120-24SC	A1
		DGS-3120-24SC-DC	A1
		DGS-3120-48TC	A1
Runtime: v1.00.028 PROM: v1.00.007	29-Sep-10	DGS-3120-24TC	A1

Upgrade Instructions:

Note 1: RI, EI & SI features are all included in the firmware. While upgrading, system will automatically distinguish it and enable the associated features only.
Note 2: RI only supports in HW version B1 with FW v3.00.522 and future version.
Note 3: Using the same firmware version and image type (EI/SI) in a physical stack is strongly recommended. The system might display error messages if mixing them.

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 firmware by CLI (serial port)

Connect a workstation to the switch console port and run any terminal program that can emulate a VT-100 terminal. The switch serial 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. It should be noted that upon the initial connection, there is no username and password by default.

To upgrade the switch firmware, execute the following commands:

Command	Function
download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {[unit <unit_id> | all]} {dest_file <pathname 64>}	Download firmware file from the TFTP server to the switch.
config firmware image {unit <unit_id>} <path_filename 64> boot_up	Change the boot up image file.
dir {{unit <unit_id>} <drive_id>} {<pathname 64>}	Display the information of current boot image and configuration.
reboot	Reboot the switch.

Example:

1. DGS-3120-24TC:admin#download firmware_fromTFTP 172.17.5.48 src_file Run100028.had dest_file Run100028.had

```
Command: download firmware_fromTFTP 172.17.5.48 src_file Run100028.had dest_file Run100028.had

Connecting to server.................. Done.
Download firmware..................... Done.  Do not power off!
Please wait, programming flash........ Done.
```

2. DGS-3120-24TC:admin#config firmware image Run100028.had boot_up

```
Command: config firmware image Run100028.had boot_up

Success.
```

3. DGS-3120-24TC#dir

```
Command: dir

Directory of /c:
```

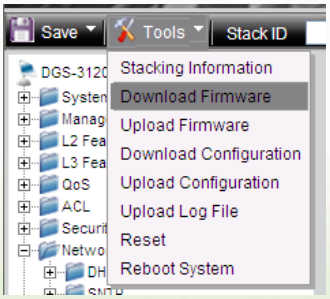
```
Idx Info     Attr Size      Update Time          Name
--- ------- ---- -------- ------------------- ----------------
  1 RUN(*)   -rw- 4881912  2000/03/17 05:27:04 Run100028.had
  2 RUN(b)   -rw- 4880456  2000/02/02 04:39:04 Run100026.had
  3 CFG(*)   -rw- 23851    2000/02/04 04:30:10 config.cfg
  4          d--- 0        2000/03/17 05:14:23 system

29618 KB total (19963 KB free)
(*) -with boot up info          (b) -with backup info
```

4. DGS-3120-24TC:admin#reboot

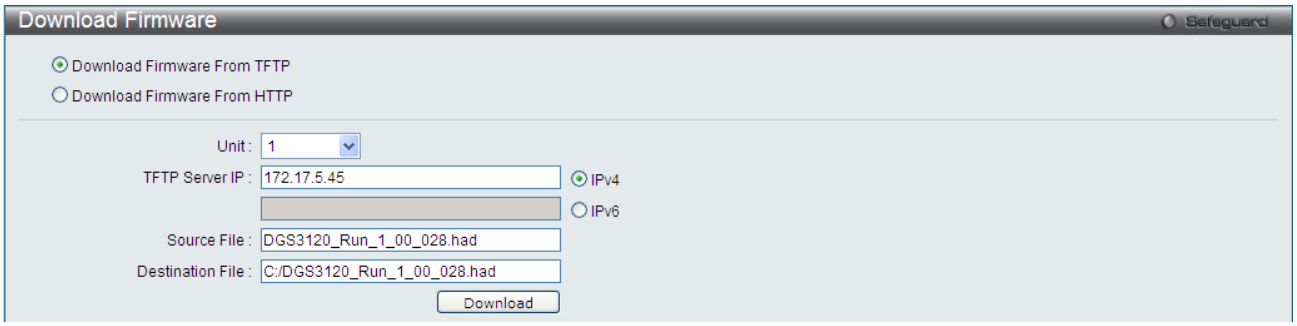
```
Command: reboot

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

  Boot Procedure                                          V1.00.007
-------------------------------------------------------------------------

  Power On Self Test ........................................  100 %

  MAC Address    : 00-40-05-31-20-00
  H/W Version    : A1

  Please Wait, Loading V1.00.028 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
  Device Discovery ..........................................  100 %
  Configuration init ........................................  100 %
```

Upgrade firmware by Web-UI

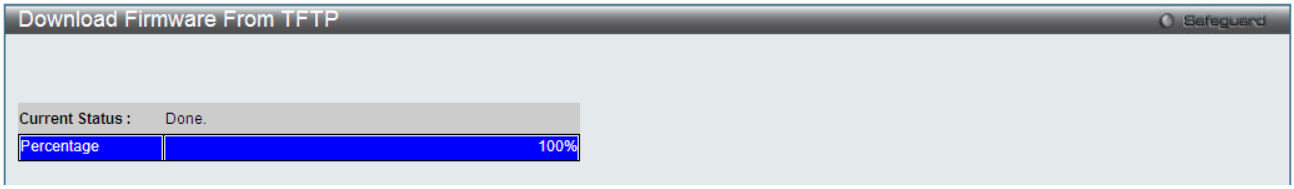
1. Connect a workstation installed with java SE runtime environment to any switch port of the device.
2. Open the web browser from the workstation and enter the IP address of the switch. The switch's default IP address is **10.90.90.90**.
3. Enter administrator's username and password when prompted. It should be noted that the username and password are blank by default.
4. To update switch's firmware or configuration file, select ***Tools > Download Firmware*** from the banner.



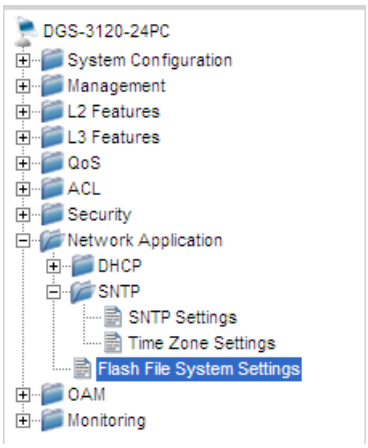
5. Enter the TFTP Server IP address.
6. Enter the name of the firmware file located on the TFTP server.
7. Enter the destination path and the desired file name.
8. Click **Download** button.

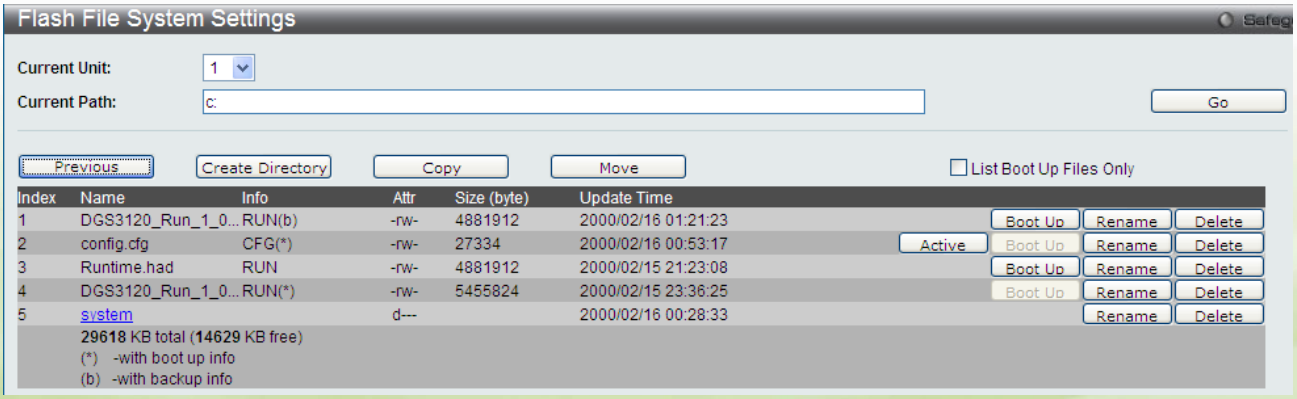


9. Wait until the Current Status displays **Done** and the Percentage shows **100%**.

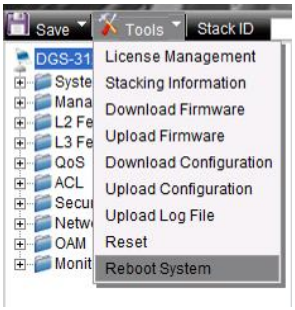


10. To select the boot up image used for next reboot, click ***Network Application > Flash File System Settings*** in the function tree and then click the ***C:*** drive name. When you see the files list, click corresponding **Boot Up** button to specify the firmware that will be used for next and subsequent boot up.

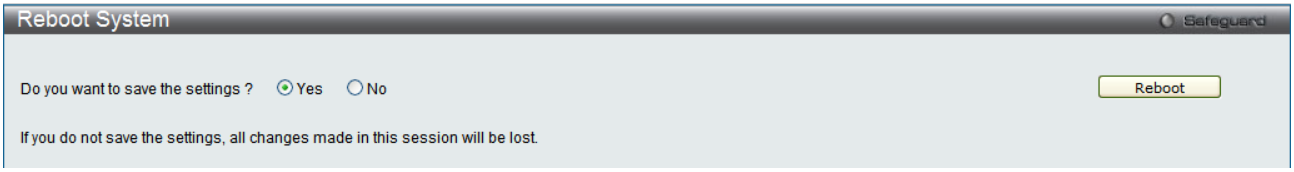




11. To reboot the switch, select ***Tools > Reboot System*** from the banner.



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



DLMS Instructions:

Some D-Link switches support DLMS (D-Link License Management System) feature. With DLMS, you can upgrade your switches to more enhanced edition to get more sophisticated features.

DLMS License Activation by CLI

Command	Function
install dlms activation_code <string 25> {unit <unit_id 1-6>}	This command is used to install an activation code to activate or unlock function on the applicance.
show dlms license {unit <unit_id 1-6>}	This command is used to display license information.

Example:

1.
```
DGS-3120-24TC:admin#install dlms activation_code DF244A4E4BC640C6394510206
Command: install dlms activation_code DF244A4E4BC640C6394510206
Success.

Please reboot the device to active the license.

DGS-3120-24TC:admin#
```

2.
```
DGS-3120-24TC:admin#reboot
 Command: reboot

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

   Boot Procedure                                          V1.00.007
 ---------------------------------------------------------------------

   Power On Self Test ....................................   100 %

   MAC Address    : 00-40-05-31-20-00
   H/W Version    : A1
```

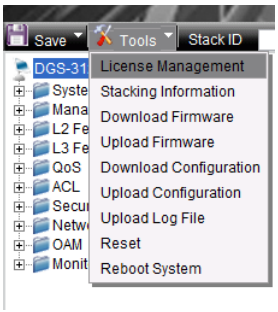
```
Please Wait, Loading V1.00.028 Runtime Image .............  100 %
UART init ................................................  100 %
Starting runtime image
Device Discovery .........................................  100 %
Configuration init .......................................  100 %
```

3. DGS-3120-24TC:admin#show dlms license

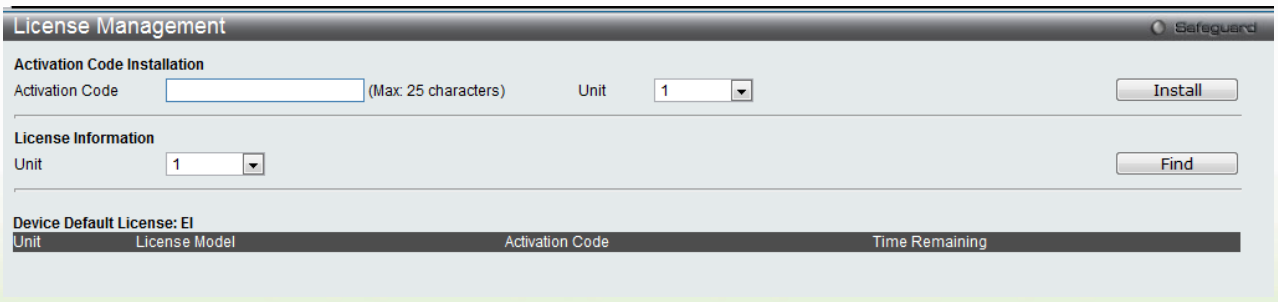
```
Command: show dlms license

Device Default License : SI

License Model              Activation Code                 Time Remaining
-------------------------------------------------------------------------------
DGS-3120-24TC-SE-LIC       DF244A4E4BC640C6394510206       No Limited
-------------------------------------------------------------------------------
                                                                  * expired
```

DLMS License Activation by Web-UI

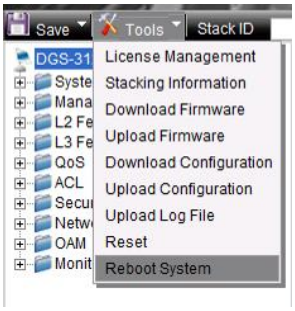
1. Connect a workstation installed with java SE runtime environment to any switch port of the device.
2. Open the web browser from the workstation and enter the IP address of the switch. The switch's default IP address is **10.90.90.90**.
3. Enter administrator's username and password when prompted. It should be noted that the username and password are blank by default.
4. To update switch's firmware or configuration file, select ***Tool->License Management*** from the banner.



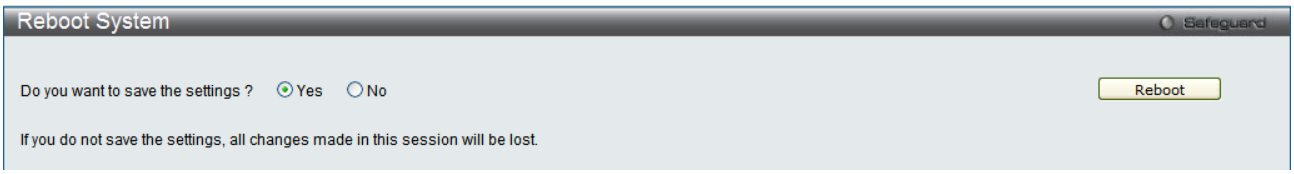
5. Enter the Activation Code and select unit of stack then click **Install** to activate the assigned switch.



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



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



New Features:

Firmware Version	New Features
v3.10.012	1. Support downloading F/W to stacking member whose HW version is different with master unit. (SI/EI) 2. Support Entity MIB. (SI) 3. Change cable diagnostic privilege level from "Power-User" to "None". (SI) 4. Support port capability advertised function. (SI) 5. Increase DHCP local rely entries to 4K. (SI) 6. Change ERPS WTR time from "5~12" to "1~12" minutes. (EI)
v3.00.522	1. Support Energy Efficient Ethernet (EEE) 2. Support Routed Image (RI) with below listed features a. DHCP server b. VRRP c. IPv6 Tunneling d. Increased routing table e. RIP f. OSPF g. IGMP h. MLD i. PIM-SM/DM/SSM/Sparse-Dense Mode j. DVMRP v3 k. **NO** support physical stacking 3. EI and SI have the same features with V3.00.022.
v3.00.022	1. Move below IPv6 features from EI to SI a. IPv6 Neighbor Discovery (ND) b. CoS for IPv6 address, traffic class and flow label c. ACL Policy for IPv6 address, traffic class and flow label d. SSH over IPv6 e. WAC, MAC and JWAC support IPv6 address f. Web-based GUI, Telnet server/client, TFTP Client, BootP/DHCP Client and SNTP over IPv6 g. SNMP over IPv6 h. IPv6 Trusted Host i. IPv6 system log server j. ICMPv6 2. Support D-Link Loopback Detection v4.04 (SI)

	3. Lower the bandwidth control minimum granularity to 8Kb/s (SI) 4. Add DoS Attack Prevention (SI) 5. Add TACACS+ Accounting (SI) 6. Add DHCPv6 Relay option 37 (SI) 7. Support extension definition on DHCP relay option 82 (SI) 8. Support Weighted Cost multi-path route (EI) 9. Support IMPB IPv6 and update IMPB version to v3.96 (EI)
v2.50.015	1. D-Link Auto Surveillance VLAN 2. WRED (Weighted Random Early Detection) 3. SNTP for IPv6 (EI) 4. UDP Helper 5. MAC authentication enhancement (using MAC address as a username/password) 6. Password Encryption Enhancement 7. Per packet type threshold for traffic control 8. Support activation code input for DLMS (D-Link License Management System) 9. Support WAC/JWAC authentication page for iOS/Android devices 10. Support download config increment 11. Support the Intermediate CA Certificates and 2048 bits key for JWAC 12. Support Mac Access Control (MAC) and JWAC combination of compound authentication 13. Support Framed-IP-Address Attribute in RADIUS Accounting packets 14. Support customized default VLAN naming 15. Change the shutdown default stat of DDM module from alarm to none
v2.00.010	1. L3 control packet filtering 2. 802.1ax 3. LLDP-MED 4. Customized WAC page 5. L2 protocol Tunneling (STP BPDU, GVRP PDU, Cisco Protocols PDU) 6. Support configuring drop threshold of L2 Protocol Tunneling 7. IGMP Authentication 8. SMTP 9. D-Link Voice VLAN 2.1 10. Time-based POE 11. Enable / Disable DHCP per VLAN 12. Extended password length to 32 characters 13. IMPB V3.91 (EI) 14. WAC/JWAC forIPv6 (EI) 15. Circuit-Id insertion for PPPoE (EI) 16. 802.3ah (DULD, D-Link Unidirectional Link Detection) (EI) 17. Optical Transceiver DDM (Digital Diagnostic Monitoring) (EI) 18. DHCPv6 Client (EI) 19. DHCPv6 Relay Agent (EI) 20. Unicast NLB (EI)
v1.02.013	1. Support new models: DGS-3120-24PC, DGS-3120-48PC
v1.01.027	1. Support new models: DGS-3120-24SC, DGS-3120-24SD-DC, DGS-3120-48TC 2. Support enable/disable stacking mode of stacking ports (Port S1 and S2). When disabling stacking mode, these 2 ports can run as normal 10GE ports. 3. 802.1ag 4. Y.1731 5. Ethernet Ring Protection Switching (EI) 6. Q in Q (EI)
v1.00.028	First release. For supported features, please refer to the product specification

	and manuals for details.

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
v3.10.012	RFC2737.mib	Support RFC2737 Entity MIB
	L2mgmtDgs3120-24PC.mib L2mgmtDgs3120-24TC.mib L2mgmtDgs3120-24SC.mib L2mgmtDgs3120-24SC-DC.mib L2mgmtDgs3120-48PC.mib L2mgmtDgs3120-48TC.mib	Support port capability advertised.
	CableDiag.mib	Change privilege level of cable diagnostic command from power user to none
v3.00.522	McastProxy.mib	Support IGMP/MLD proxy
	DHCPServer.mib	Support DHCP server
	l3mgmt.mib	1. Support IP directed broadcast 2. Support loopback/null interface 3. Support static IP multicast route
	RFC2787.mib	Support VRRP
	RFC4087.mib	Support IPv6 tunneling
	PolicyRoute.mib	Support policy based route
	RFC1724.mib	Support RIP
	RIPNG.mib	Support RIPng
	RFC1850.mib	Support OSPF
	RFC5643.mib	Support OSPFv3
	IGMPv3.mib	Support IGMP
	RFC5519.mib	Support MLD
	RFC2934.mib	Support PIM-DM
	PIM-SM.mib	Support PIM-SM/SSM/ Sparse-Dense Mode
	RFC5060.mib	Support PIM for IPv6
	dvmrp.mib	Support DVMRPv3
v3.00.022	LDB.mib	Support D-Link Loopback Detection 4.04
	Qos.mib	Modify bandwidth minimum granularity from 64Kbps to 8Kbps
	SSH.mib	Support uploading user's public key for SSH
	PortSecurity. mib	Support port shutdown action when it over max learning address

	Dosprev.mib	Support DoS attack prevention
	AAC.mib	Support TACACS+ accounting
	l3mgmt.mib	Support DHCPv6 Option 37
	DHCPRelay.mib	1. Support Extension definition on DHCP option 82 Circuit ID 2. Support DHCP relay option 37
	IPMacBind.mib	1. Support IPv6(IPv6 ND snooping&IPv6 DHCP snooping) 2. Support D-Link IMPB V3.96 that provides IP DHCP Snooping limit rate to prevent DHCP attacking.
v2.50.015	SSL.mib	Support the Intermediate CA Certificates and 2048 bits key for JWAC
	AUTH.mib	Support compound authentication for MBA and JWAC
	DLMS.mib	Support DLMS (D-Link License Management System)
	Surveillance_VLAN.MIB	Support D-Link Auto Surveillance VLAN
	wred.mib	Support WRED (Weighted Random Early Detection)
	Time.mib	Support SNTP for IPv6
	UDPHelper.mib	Support UDP Helper
	mba.mib	MAC authentication enhancement (MAC authentication using MAC address as a username/password)
	Q-Bridge.mib	Support customized default VLAN naming
	Genmgmt.mib	1. Download config increment 2. Password Encryption Enhancement
	DDM.mib	Change the shutdown default state of DDM module from alarm to none.
	PktStormCtrl.mib	Per packet type threshold for traffic control
v2.00.010	NLB.mib	Support unicast NLB
	IEEE8023-LAG-MIB.mib	Support 802.1ax
	L2mgmt.mib	Disable a VLAN trunk member port
	LLDP-MED.MIB	Add LLDP-MED
	lldp.mib	To take system IP address into LLDP management IP interface configuration
	L2ProtocolTunnel.mib	1. Support tunneling STP BPDU 2. Support tunneling GVRP PDU 3. Support tunneling Cisco Protocols PDU across provider network 4. Support configuring drop threshold of L2 Protocol Tunneling
	VoiceVLAN.mib	Support configuring port join voice VLAN

		as tag or untag member
	Filter.mib	Support RPC port mapper filter Support L3 control packet filter
	L2mgmtDgs3120-24PC.mib L2mgmtDgs3120-24SC.mib L2mgmtDgs3120-24SC-DC.mib L2mgmtDgs3120-24TC.mib L2mgmtDgs3120-48PC.mib L2mgmtDgs3120-48TC.mib	Support IGMP Authentication
	Auth.mib	Support VLAN-based authentication for JWAC
	Jwac.mib	Add IPv6 JWAC support for EI
	wac.mib	1. Support customized pages 2. Support dynamic ACL assignment 3. Add IPv6 WAC support for EI
	AAC.mib	Support user authentication & authorization by TACACS+
	smtp.mib	Add SMTP support
	l3mgmt.mib	1. Add DHCPv6 Client for EI 2. Support enable/disable DHCP Relay per VLAN 3. Support DHCP Relay Option 12
	DHCPv6Relay.mib	Add DHCPv6 Relay Agent for EI
	PPPoEmgmt.mib	Support Circuit-Id insertion
	DDM.mib	Add DDM for EI
	Duld.mib	1. Support DULD based on 802.3ah OAM 2. Support following dying gasp PDUs and traps: Device reboot, All fan fail
	Equipment.mib	Support scheduled on/off LED
	PoE.mib	Support scheduled on/off POE
v1.02.013	ie8023ah.mib	Add 802.3ah for EI
	PoE.mib	Add PoE feature
v1.01.027	DHCPRelay.mib	Add DHCP relay VLAN table for SI
v1.00.028	First release. Please refer to datasheet for supported SNMP MIB files.	

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
v3.10.012	1. config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc

	1-32> | clear_description]} changes to config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | auto_negotiation [restart_an | remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description] | auto_speed_downgrade [enable | disable]} 2. config erps raps_vlan <vlanid 1-4094> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid 1-4094> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid 1-4094> | revertive [enable| disable] | timer { holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000 > | wtr_time <min 5 - 12>}] changes to config erps raps_vlan <vlanid 1-4094> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid 1-4094> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid 1-4094> | revertive [enable| disable] | timer { holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000 > | wtr_time <min 1 - 12>}] 3. config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip [<ipaddr> | none] | remap_priority [<value 0-7> | none] {replace_priority}}(1) changes to config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip [<ipaddr> | none] | remap_priority [<value 0-7> | none] { replace_priority} | cvid [<vlanid 1-4094> | null]}(1) 4. config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 [<ipv6addr> | none] | remap_priority [<value 0-7> | none] {replace_priority}}(1) changes to config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 [<ipv6addr> | none] | remap_priority [<value 0-7> | none] {replace_priority} | cvid [<vlanid 1-4094> | null]}(1)
v3.00.522	None
v3.00.022	None
v2.50.015	None
v2.00.010	1. config igmp_snooping [vlan_name <vlan_name 32> | vlanid

	<vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable]} changes to config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] { state [enable | disable] | fast_leave [enable | disable] | proxy_reporting {state [enable|disable] | source_ip <ipaddr>}(1)}
v1.02.013	None
v1.01.027	1. config dhcp_relay add ipif <ipif_name 12> <ipaddr> config dhcp_relay delete ipif <ipif_name 12> <ipaddr> changes to config dhcp_relay add vlanid <vlan_id_list> <ipaddr> config dhcp_relay delete vlanid <vlan_id_list> <ipaddr> **Note:** These commands are changed only in SI, and stay unchanged in EI. 2. create access_profile profile_id <value 1-768> … delete access_profile profile_id <value 1-768> … config access_profile [profile_id <value 1-768> | …] [add access_id [auto_assign | <value 1-1536>] … changes to create access_profile profile_id <value 1-6> … deletete access_profile profile_id <value 1-6> … config access_profile [profile_id <value 1-6> | …] [add access_id [auto_assign | <value 1-256>] … 3. create egress_access_profile profile_id <value 1-256> … delete egress_access_profile profile_id <value 1-256> … config egress_access_profile [profile_id <value 1-256> | …] [add access_id [auto_assign | <value 1-512>] … changes to create egress_access_profile profile_id <value 1-4> … delete egress_access_profile profile_id <value 1-4> … config egress_access_profile [profile_id <value 1-4> | …] [add access_id [auto_assign | <value 1-128>] …
v1.00.028	First release

Problem Fixed:

Firmware Version	Problems Fixed
v3.10.012	1. The slave member port cannot learn FDB entries if user added it by VLAN name and enabling voice VLAN in stacking system. **(DEUR20121220000001)** 2. The JWAC client could not get IP address from DHCP server when enable JWAC UDP filtering and IMPB also were enabled on other port. **(DI20130121000003, DI20130227000001)** 3. Correct the incorrect spelling "Temperatrue" in log. **(DRU20130124000005)** 4. The IMPB DHCP snooping maximum entry setting does not work as configured. **(DRU20130130000008)** 5. SSH session responses slowly when displays port/interface information **(DI20130704000006)** 6. The looped ports did not be blocked when it happened on the combo ports. **(DEUR20130702000004)** 7. The web GUI did not show flash file system correctly on IE10 and Chrome. **(DI20130717000008)**

	8. DGS-3120-24SC will auto reboot if user uses SNMP to set "swL2PortCtrlNwayState" under DGS3120-24SC-L2MGMT-MIB tree. **(DRU20130723000003)** 9. The device did not send the traps when OAM detected error frame. **(DRU20130917000001)** 10. The CPU utilization may become high after power on/off device 30~200 times. It will cause ping loss and Web-UI response will be extremely slow or no response. **(DUSA20131003000001)** 11. User cannot set bandwidth control by TX/RX rate on stacking member through Web UI. **(DEUR20131007000004)** 12. When enables DHCP relay and STP at the same time, DGS-3120 will flood the DHCP ACK or NAK packets to all ports and causes DHCP broadcast storm **(DGC20130913000001)** 13. DGS-3120 may suddenly reboot while GPIO semaphore was occupied by other low priority task. **(DI20130924000003)**
v3.00.522	None
v3.00.022	1. Stacking member enters exception error mode after entering command "create cfm mep". **(DI20110118000006)** 2. The port connects to Intel 10G Adapter (product code: EXPX9502CX4) through DEM-CB300CX will not link up after reboot. **(DRU20110422000003)** 3. Multicast stream flooded incorrectly if multicast filtering mode for VLAN set as filters unregistered groups when MLD/IGMP enabled globally and MLD/IGMP disabled at VLAN as well. **(DI20110616000002)** 4. Multicast stream did not forward after slave switch rebooted. **(DI20110617000015)** 5. DGS-3120-24PC per port power limit default setting should be 15400mW but not 7000mW. **(DI20110628000011)** 6. Double tagged IGMP query cannot go through the ports. **(DEUR20110616000006)** 7. DGS-3120 did not send calling station id to RADIUS server caused MAC-based access control authentication through RADIUS will fail. **(DUSA20110628000001)** 8. The traffic segmentation function doesn't work correctly when link aggregation enabled at the same time. **(DRU20110708000001, DRU20111111000002, DEUR20121002000010)** 9. In stacking mode, DGS-3120 will change source MAC address for BPDU after powering off link partner which connect to slave switch. **(DI20110714000009)** 10. In stacking mode, DGS-3120 uses incorrect source MAC address for LACPDU. **(DI20110714000009)** 11. DGS-3120 changes source MAC address of LACPDU after the master switch re-election. **(DI20110714000009)** 12. DGS-3120 carries wrong user name in 802.1X accounting when using MAC/Linux OS with PEAP+MSCHAPv2 for the outer identification. **(DEUR20110802000002)** 13. DGS-3120 may hang up when receiving a lot of DHCP discovery packets and cannot access the switch via web UI or telnet. **(DRU20110801000001)** 14. DGS-3120 RADIUS accounting cannot work correctly when more than one client (supplicant) connected to the same port with enabling host-based 802.1X authentication. **(DEUR20110805000001)** 15. DGS-3120 cannot show WAC/JWAC authentication/logout page correctly with WIN7, IE9, Firefox and Chrome. **(DI20110913000003, DI20111209000009, DI20111209000008)** 16. DGS-3120 does not transmit DHCP "release" packet when DHCP relay is enabled. **(DEUR20110919000004)**

17. When the outer TPID is the same as inner TPID(0x8100), the switch will incorrectly recognize the incoming packets as outer tagged packets and drops the packets. **(DRU20110923000002)**
18. Authentication log out page cannot be accessed if WAC virtual IP is not set. **(DI20111003000006)**
19. There is no entry of changing command prompt when entering "show config modified". **(DEUR20111003000001)**
20. File in the SD card will disappear after renaming the directory of that file. **(DI20111014000004)**
21. The "Radius Stop" message will has incorrect port id "0" when the clients under the port with 802.1X enabled moved to the other port with 802.1X authentication disabled.**(DEUR20110919000002)**
22. WAC for IPv6 does not work if system IP interface for IPv4 is disabled or set to 0.0.0.0/0 even though system IP interface for IPv6 is enabled. **(DI20111027000005)**
23. If DGS-3120 configured two IP interfaces will cause it cannot respond trace-route command correctly. **(DRU20111028000005)**
24. Clients may not get the configuration from DHCP server and the sessions of telnet delayed when CPU utilization rise to 100% after enabling DHCP relay and DHCP relay option 82. **(DRU20110830000006)**
25. The serial port baud rate will change back to default value, 115200, after reboot the switch. **(DEUR20111207000004)**
26. In stacking mode, DGS-3120 will send two duplicate DHCP offer packets when DHCP snooping is enabled. **(DI20111209000005)**
27. DGS-3120 does not redirect to IPv6 WAC authentication HTTPS page. **(DI20111209000010, DI20111209000011)**
28. DGS-3120 discards OSPFv3 "hello" packets from a VLAN's port which multicast packets filtering mode set as filter unregistered multicast groups. **(DI20111215000006)**
29. The inner tag is not excluded from packet when egress port's role is UNI port. **(DRU20111221000001)**
30. When master switch power off, the ERPS state will not enter protection mode and caused packets dropped. **(DI20111226000002)**
31. DGS-3120 will delete IGMP snooping group when a client joins an invalid IGMP snooping group. **(DRU20111220000003)**
32. There are 4 groups reserved octets of LACPDU packet should be zero as standard IEEE 802.1AX-2008 defined. These octets reserved for use in future extensions to the protocol and shall be ignored on receipt. **(DRU20111223000001)**
33. The multicast packets are dropped when there is port status change for other member ports in the same group. **(DEUR20111209000013)**
34. When master switch is down, DGS-3120 will discard IGMP/MLD general/specific query from the LACP port which IGMP/MLD snooping enabled. **(DI20120111000014)**
35. The mirror port cannot capture RADIUS (EAP) traffic from the source port which belongs to different stacking units. **(DUSA2012012000001)**
36. There will be oversize error on 10G port when enable jumbo frame. **(DRU20120208000002)**
37. After entering the command "config poe ports all state disable", the switch will not display the changed command when executing "show config modified". **(DI20120131000008)**
38. If the switch enables PPPOE circuit ID insertion, the switch will not respond ping packet and cannot access it. **(DRU20120215000005)**
39. The "cfm loopback" test will be failed when only slave switch has an active link. **(DI20120229000004)**
40. The counter displays incorrect value for traffic control threshold. **(DI20120302000005)**

41. The MEP port status should display "port blocked" when the remote MEP port is link down, but the switch always display "port up". **(DEUR20120408000001)**
42. LED admin state is incorrect. The LED should be shut down when admin state disable. **(DI20120410000010)**
43. In JWAC, the switch did not force IPv6 client to log out when hop limit value equals to 1 in ICMP packet. **(DI20120418000008)**
44. The CFM MEP status of the switch is different from CFM remote MEP status. **(DI20120416000003)**
45. DGS-3120 forwarded CFM frames incorrectly from a port which was blocked by STP. **(DI20120424000003)**
46. When executes "show cfm ports" command; switch displays incorrect MAC address of the port which is not belong to the unit 1 switch in the stack. **(DI20120427000004)**
47. The web page size is too large for each WAC/JWAC authentication session; some authentication entries will fail if any packet is lost. **(DI20120416000002, DI20120523000006)**
48. Power saving by system hibernating does not work in the stacking mode. **(DI20120413000002)**
49. The port will lose connection when 802.1X authentication session time out because of DGS-3120 only sent EAP failure packets and did not send EAP request packets. **(DI20120424000001)**
50. DGS-3120 does not reply correct firmware version to SNMP server when it sends SNMP get request to DGS-3120. **(DI20120511000006)**
51. User cannot access to DGS-3120 via SSH with host-based authentication mode. The switch always returns error message "Permission denied". **(DEUR20120327000009)**
52. When box-id is not 1 in standalone mode, DGS-3120 sent packets with wrong source MAC address for BPDU. **(DI20120515000005)**
53. CFM cannot work correctly when enables ERPS at the same time. **(DRU20120511000002)**
54. The switch can't get LLDP remote information on the ERPS RPL port. **(DRU20120516000004)**
55. The LLDP and CFM-CCM packet did not send with master's unit ID of stack after the unit is down. **(DI20120611000008, DI20120615000008)**
56. DGS-3120 cannot configure multiple mirror groups. **(DRU20120605000003)**
57. If the LACP member ports belong to different stacking units, the stacking may not be established after rebooting slave switch. **(DEUR20120530000005)**
58. The master switch may not forward BPDU packets to slave switch in time when used "save" command and caused STP topology changed on salve switch. **(DLA20120628000001)**
59. The switch cannot configure port mirror via Web UI. **(DRU20120625000003)**
60. When upgrade firmware type from SI to EI, the firmware type still is SI when executes "show switch" command. **(DGC20120712000001)**
61. When user connects untagged ports between different VLAN and enables LBD function, the switch incorrectly detects loop. **(DI20120709000009)**
62. The SNMP IF-MIB OID "ifInUcastPkts" will re-count from 0 if counter's value is over 2^{26}. **(DRU20120724000004)**
63. The DHCP offer packets will be dropped when enabling DHCP local relay in private VLAN. **(DRU20120807000011)**
64. The outer TPID will be changed to 0x88a8 from 0x8100 when enables Q-in-Q then the telnet connection is lost since NIC can't recognize the TPID with 0x88a8. **(DRU20120725000001)**
65. User cannot see the mirrored traffic from the 2nd mirror group.

	(DGC20120815000003) 66. DGS-3120 doesn't forward DHCP offer packet to client with DHCP relay per VLAN configuration. It causes clients cannot obtain the IP address. **(DRU20120815000001)** 67. User cannot change TPID for any port before enabling Q-in-Q via web UI. **(DRU20120828000002)** 68. When DGS-3120 receiving the "dying gasp" message from OAM, the associated trap is not triggered. **(DEUR20120830000007)** 69. DGS-3120 proxy reporting function does not work correctly. **(DEUR20120919000005)** 70. IGMP snooping configuration for non-default VLAN cannot be changed via web UI. **(DEUR20120919000004)** 71. Switch doesn't show MAC address in FDB table with dynamic VLANID. **(DRU20120913000002)** 72. DGS-3120 sends DHCP offer packet with all zero in source MAC address will cause some devices cannot obtain the IP address. **(DRU20120926000002)** 73. The role of switch has not been reselected when disabled the STP of port. **(DLA20121009000003)** 74. DGS-3120 cannot be accessed through IP interface and ISM VLAN did not work. **(DRU20121003000005)** 75. After rebooting DHCP client which connect to the link partner, DGS-3120 will drop DHCP discover packet if enabling DHCP local relay and address binding function at the same time. **(DEUR20121016000001)** 76. DGS-3120 will reboot automatically when running the SSH attack tool. **(DI20121012000007)**
v2.50.015	1. The command "clear mac_based_access_control auth_state ports all" may cause LCAP link unstable, due to DGS-3120 doesn't send LACPDU for 5 seconds during clear 1,000 MBA auth_entry. **(DI20110615000008)** 2. The command "clear wac auth_state ports *" may cause LCAP link unstable due to DGS-3120 doesn't receive/send the LACPDU during clear 1,000 MAC in WAC authentication and WAC compound authentication. **(DI20110705000009, DI20110705000010)**
v2.00.010	1. In a DGS-3120 stack, the loop condition will happen on some VLAN though it should be blocked by MST, when Master unit cold restart. 2. When reboot member unit of stack, it will show a lot of error messages like following: "snp_stk_process_tx_drop_counter> fatal error, index : 1 , vid = 2020". **(DI20110225000002)** 3. When issued "show ipv6 neighbor_cache ipif" command, DGS-3120 incorrectly displayed many entries. **(DI20110420000011)** 4. When LACP function has been configured or modified, and then issue command "show config effective" or "show config modify", the output is empty. 5. DGS-3120 member unit entered exception mode in a few days after Link down & up several times within a short period. **(DI20110124000003)** 6. The MAC address of LLDP per port is incorrect. **(DRU20110512000003)** 7. DGS-3120 supports temperature MIB, but swEquipmentCapacity incorrectly returned "no capacity". **(DI20110411000001)** 8. When stacking mode was enabled and then disabled, SNMPWALK swUnitMgmtModuleName incorrectly return value of stacking mode. **(DI20110411000001)** 9. DGS-3120 incorrectly sends MLD general query with source MAC of all zero after link up. **(DI20110406000008)** 10. DGS-3120 cannot communicate to IPv6 client by IPv6 link local address. **(DI20110309000008)** 11. DGS-3120 enters exception mode after power down member unit with IGMP

	Snooping configured. **(DI20110228000006)** 12. DGS-3120 do not forward multicast stream to client on non-stp ports when STP is enabled. **(DI20110228000007)** 13. The STP role is always "NoSTP" when the port enable STP and LACP. **(DI20110322000002)** 14. In stacking mode with configured LACP, the LACP active ports will be incorrect show turn-off, when turn on/off the master/member units. **(DRU20110128000003)** 15. Stacking status is not synchronous when ERPS sub-ring was changed. **(DI20110401000012)** 16. When switch enable stacking and configured ERPS, packet loop happened after reboot **(DI20110228000004)** 17. When topology change of ERPS, DGS-3120 do not clear IPFDB, and IP communication stopped **(DI20110208000003)** 18. Packets loop happened after stack member unit reboot of ERPS RPL Owner. **(DI20110202000006)** 19. After member unit reboot, the ERPS state of member unit is different from master. **(DI20110203000002)** 20. When some STP port is disabled, it takes about 30 seconds to complete MST convergence after topology changed. **(DI20110118000007)** 21. IPv4/v6 Multicast Query packets were forwarded from the Blocking port in sub-ring when IGMP/MLD Snooping is enabled. **(DI20110120000005)**
v1.02.013	1. When configuring the multicast filtering mode on filter_unregistered_groups, the IPv6 clients cannot get link local IP correctly. 2. DGS-3120 does not converge after CIST priority was changed. **(DI20101228000001)**
v1.01.027	1. In a DGS-3120 stack, if there are over 4,000 active VLANs and also a cross-stack trunk is connected, the switch will not send BPDU and LACP control packets through the cross-stack trunk ports within a few seconds when executing some commands such as "save", "show config current_config", or "show tech_support". **(DI20100525000005)** 2. In a DGS-3120 stack, if there are over 4,000 active VLANs and also a cross-stack trunk is connected, the switch will not send BPDU and LACP control packets through the cross-stack trunk ports within a few seconds when one of the stacking member is rebooting or the stacking master is suddenly powered off. **(DI20101109000004), (DI20101109000009), (DI20101109000005)** 3. In a DGS-3120 stack, if there are over 4,000 active VLANs and also a cross-stack trunk is connected, the switch will send a duplicate TCN through cross-stack trunk ports for about 30 seconds after topology stabilized. 4. When there are over 50 WAC clients keeping login/logout for few hours, some clients may fail to login. **(DI20101119000005)** 5. If there are a lot of WAC clients keeping login/logout and WAC function is suddenly disabled, the switch will get into exception mode. 6. DGS-3120 failed to operate the SD card with FAT16 file system. **(DI20101112000001)** 7. It takes over 30 seconds to change the STP port status from discarding to forwarding if the received BPDU is with CIST remaining hop count = 0. **(DI20101111000004)** 8. Some counter values in IF-MIB are not correct. **(DI20101110000009)** 9. When flash memory is full, all the file names in file system will be garbled **(DI20101112000003)** 10. When disabling SSL setting for switch Web UI, SSL WAC clients cannot correctly access the WAC login page via https. 11. The storm control settings does not take effect if the port is STP enabled and also connects to a looped network.

	12. If failing to copy a file to SD card and rebooting the switch right after that, the switch enters exception mode. **(DI20101125000010)** 13. Error spelling in DHCP Snooping Entry setting page of Web UI. **(DI20101202000009)** 14. DHCP relay function does not work in SI. **(DRU20101130000004)** 15. When continuously executing "show wac auth_state ports" or "show arpentry" command for a period of time, the screen of console will hang up. **(DI20101210000005)** 16. If authenticating consecutive MAC addresses via Mac Access Control (MAC) and RADIUS database, DGS-3120 will have 5 seconds delay sending every authentication packet to RADIUS. **(DI20101208000008)** 17. If executing "reset config" command when the switch is undertaking Mac Access Control (MAC) authentication against clients, the switch will enter exception mode. 18. When over 1,000 clients are authenticated through WAC in Compound Authentication, some clients will be blocked by the switch. **(DI20101208000005)** 19. When authenticating over 120 clients using Compound Authentication at the same time, some clients failed to authenticate. **(DI20101207000009)** 20. DGS-3120 does not mirror BPDU TX packet if setting the mirror target port on different units of the stack. **(DI20101130000010)**

*** D-Link tracking number is enclosed in ()**

Known Issues:

Firmware Version	Issues	Workaround
v3.10.012	1. This firmware version cannot be installed on HW version B1.	Please install V3.10.512 on HW version B1.
	2. If user creates 4K VLANs and enables MSTP, LACP at the same time; the CPU utilization will remain high if there's status change for MSTP forwarding port.	No workaround. It is HW limitation and will not affect the tasks with high priority.
v3.00.522	1. This version cannot install on HW version A1/A2.	Please install v3.00.022 on HW version A1/A2.
v3.00.022	None	None
v2.50.015	1. It cannot upgrade to v2.50 from v1.02 or earlier firmware	Please upgrade to v2.00 first before upgrading to v2.50
	2. Switches do not limit EI/SI devices put in the same stack. However, if the master is EI and some slaves are SI, the slave switch may return error messages for some EI commands.	Only put the devices with the same edition (SI/EI) into the stack.
v2.00.010	None	None
v1.02.013	None	None
v1.01.027	1. The number of ingress ACL profile changes from 768 to 6 and egress ACL profile changes from 256 to 4. However, the total number of ACL rules remains the same.	In order to save profile usage, use longer ACL profile to cover the same type of ACL rules. For example, rules inspecting MAC address, VLAN, or 802.1p respectively, which all belong to MAC ACL, can make use of only one profile that masks MAC address, VLAN, and 802.1p.
	2. In previous firmware release, the ACL	Please review the profile ID settings

	sequence is MAC ACL > IP ACL > IPv6 ACL > User Defined ACL. After v1.01.027, the ACL sequence will depend on the ACL profile ID. ACL rules with Lower profile ID will get higher priority.	before upgrading F/W from v1.00.xxx to v1.01.027 or later version.

Related Documentation:

- DGS-3120 Series Web UI Reference Guide Release 3.10
- DGS-3120 Series CLI Reference Guide Release 3.10
- DGS-3120 Series A1/A2 Hardware Installation Guide Release 3.10