



Firmware Version: v2.00.B27
Prom Code Version: v1.00.B06
Published: 2009/1/13

These release notes include important information about D-Link switch firmware revisions. Verify that these release notes are correct for your switch:

- If you are installing a new switch, check the hardware version on the device label; make sure your switch meet the system requirement of this firmware. See [Revision History and System Requirement](#) for detailed firmware and hardware matrix
- If your switch is on, check the hardware version by using “show switch” command or see the device information page on web graphic user interface
- If you are upgrading to a new release firmware, see the [Upgrading Instructions](#) to make sure the firmware upgrade procedure is correct.

For the detailed information of the switch products, see [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
Upgrading Instructions:	2
Upgrading by using CLI (serial port)	2
Upgrading by using Web-UI	2
New Features:	5
Changes of MIB & D-View Module:	7
Changes of Command Line Interface:	8
Problem Fixed:	8
Known Issue:	9
Related Documentation:	10

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
Runtime: v2.00.B27 Prom: v1.00.B06	2009/1/13	DES-3028	A1
		DES-3028P	A1
		DES-3028G	A1
		DES-3052	A1
		DES-3052P	A1
Runtime: v1.00.B32 Prom: v1.00.B04	2007/04/12	DES-3028	A1
		DES-3052	A1
		DES-3028P	A1
		DES-3052P	A1

Upgrading Instructions:

Upgrading by using CLI (serial port)

- Download firmware from D-Link web site <http://tsd.dlink.com.tw> and put the download firmware to TFTP server directory path.
- Access the switch via the serial port.
- The Switch's serial port's default settings are as follows:
 - Baud rate: **9600**
 - Data bits: **8**
 - Parity: **None**
 - Stop bits: **1**
- A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above are then connected to the Switch's serial port via an RS-232 DB-9 cable.
- Connect computer to the switch via RJ45 network cable and enable TFTP server on the computer.
- Enter administrator's username and password, which are blank by default.
- Syntax: download firmware_fromTFTP <ipaddr> <path_filename 64> {image_id <int 1-2>}
 - Eg: DES-3028: 4#download firmware_fromTFTP 10.90.90.91 des30xpp_runtime_v2.00.b27.had image_id 1
- Type "show firmware information" to confirm the next boot up firmware version.
- If the loaded firmware exists in image id 1, change the boot up image from id 1
- Syntax: config firmware image_id <int 1-2> [delete | boot_up]
 - Eg: DES-3028: 4#config firmware image_id 1 boot_up
- Reboot the switch, DES-3028: 4#reboot
- Type "show switch" to verify the firmware version.

Upgrading by using Web-UI

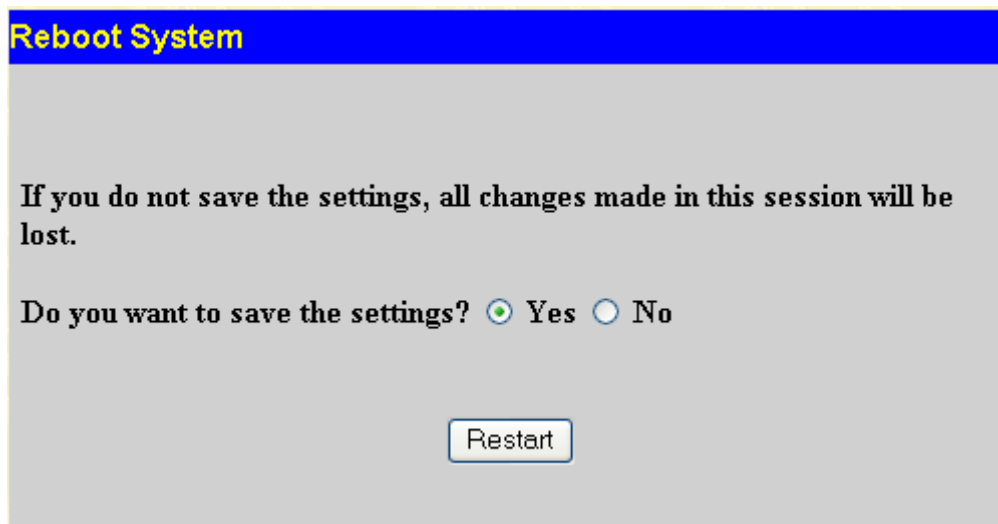
- Download firmware from D-Link web site <http://tsd.dlink.com.tw> and put the download firmware to TFTP server directory path.
- Download java SE runtime environment and install on your computer.
- Accessing the switch via System IP address, 10.90.90.90 is the default System IP

- address.
4. Confirm that your computer can access the switch via RJ45 network cable.
 5. Enable TFTP server on the computer.
 6. Enter administrator's username and password, which are blank by default.
 7. To update the switch's firmware or configuration file, click **Administration > TFTP Services**
 - Active: Select **Download Firmware**
 - Server IP Address: Enter TFTP server IP address
 - File Name: Enter the download firmware file name which located on TFTP server
 - Image ID: To select an image ID which the firmware file will be transferred

8. Enter "Start" button.
9. Wait for file Transfer to reach 100% and program firmware status completed.

10. To select the image which you want to boot up while the switch reboots next time, click **Administration > Multiple Image Services**

11. Reboot the switch, click *reboot system*
12. Click restart button.



13. Verify firmware version, go back to home page: *Web Management Tool*

New Features:

Fireware Version	New Features
v2.00.B27	<ol style="list-style-type: none"> 1. Support new model DES-3028G 2. 802.1D 2004 edition 3. Root Restriction (defined in 802.1Q-2005) 4. MLD Snooping v1 and v2 awareness 5. DoS attack Prevention 6. Asymmetric VLAN 7. IP-MAC-Port Binding v3.3 8. IMPB auto recovery 9. ISM VLAN 10. IGMP authentication 11. VLAN trunking 12. Loopback detection v2.0 13. Support Port-based QinQ (TPID of outer tag cannot be configured to 0x8100) 14. LLDP 15. Cable Diagnostics 16. Gratuitous ARP 17. Password encryption 18. Extend trusted host number to 10 entries and add mask function on trusted host 19. Support data driven multicast learned automatically 20. Support limited IP multicast address ranges 21. Product serial number can be displayed on GUI, CLI and be queried via SNMP. (From new shipment and burn-in serial number in H/W) 22. Password Recovery v1.1 23. Support VLAN batch configuration 24. Be able to force the 802.1X client to go offline 25. Support 802.1X session timeout attribute 26. Can assign ingress/egress bandwidth control and 802.1p priority to the port according to the attributes dispatched from Radius Server 27. Support "show tech support" command for troubleshooting 28. Support configurable MDI/MDIX, it can be manual configure as Auto, Normal and Cross mode 29. Remark DSCP to 802.1p priority tag 30. Extend dynamic VLAN groups to 255 31. Support three MAC address format: 11-22-33-44-55-66, 11:22:33:44:55:66 or 112233445566 32. Add auto complete commands with extra parameter "force_agree". Instead of popping up (Y/N) message while enter reset and reboot, it will be executed automatically 33. Remove all ACL entries by one command in CLI, Web and SNMP 34. Remove all trust host entries by one command in CLI, Web and SNMP

Fireware Version	New Features
V2.00.B27	<ul style="list-style-type: none"> 35. Display remaining ACL rules on Web/CLI 36. Add a SNMP MIB to support VLAN advertisement enable/disable function 37. Add show memory usage/percentage SNMP MIB 38. Add an OID to show port utilization 39. Add an OID to clear FDB and ARP table 40. Add ping command to user privilege 41. Stop contacting to TACAS+ server periodically before logging-in 42. Add "show VLAN" command by VLAN ID 43. Add "show FDB VLAN" command by VLAN ID 44. Support tagged ports column while show VLAN 45. Support forbidden router port 46. Add the ability to forward the unregistered multicast traffic to router port even when the 'filter unregistered groups' option is enabled. 47. Add RFC2869 RADIUS extension standard to get 64 bits counters from two attribute "Acct-Input-Gigawords & Acct-Output-Gigawords" 48. Support to get NAS-ID from switch "system name" and can be configure NAS-ID 49. Support DHCP relay option 82 remote ID 50. Support DHCP local relay to insert option 82 information on DHCP broadcast packets in client's VLAN 51. Block broadcast packet in DHCP relay 52. Ability to set the row number of terminal line 53. Add ARP-FDB table for easy set static entry to IP_MAC_Port binding tables 54. Extend ACL access id number from 256 to 65535 55. Remove the display of MAC address from telnet log 56. Support broadcast storm control port shutdown log 57. Support port information on STP log event while STP topology changes. 58. DLF rename to Unicast in storm control feature 59. Redirect embedded URL of D-Link logo to local OBU web site. 60. Remove Web-UI welcome page
v1.00.B32	First release, please refer to datasheet and manual for detail function supported

Changes of MIB & D-View Module:

The new features of MIB file are also included in the corresponding D-View module. Please download the MIB and D-View module on <http://tsd.dlink.com.tw>.

Firmware Version	MIB File	New Features
v2.00.B27	ACL.mib	<ol style="list-style-type: none"> 1. Remove all ACL entries by one command in CLI, Web and SNMP 2. Remark DSCP to 802.1p priority tag
	Genmgmt.mib	<ol style="list-style-type: none"> 1. Remove all trust host entries by one command in CLI, Web and SNMP 2. Extend trusted host number to 10 entries and add mask function on trusted host 3. Add show memory usage/percentage SNMP MIB 4. Add an OID to show port utilization 5. Add an OID to clear FDB and ARP table 6. Product serial number can be displayed on GUI, CLI and be queried via SNMP. (From new shipment and burn-in serial number in H/W)
	MSTP.mib	<ol style="list-style-type: none"> 1. 802.1D 2004 edition 2. Root Restriction (defined in 802.1Q-2005)
	des3028-L2mgmt.mib, des3028p-L2mgmt.mib, des3052-L2mgmt.mib, des3052p-L2mgmt.mib, des3028g-L2mgmt.mib	<ol style="list-style-type: none"> 1. Add a SNMP MIB to support VLAN advertisement enable/disable function 2. Support forbidden router port 3. Support VLAN batch configuration 4. Support configurable MDI/MDIX, it can be manual configure as Auto, Normal and Cross mode. 5. Asymmetric VLAN 6. Can assign ingress/egress bandwidth control and 802.1p priority to the port according to the attributes dispatched from Radius Server. 7. ISM VLAN 8. Support DHCP local relay to insert option 82 information on DHCP broadcast packets in client's VLAN 9. IGMP authentication 10. Add the ability to forward the unregistered multicast traffic to router port even when the 'filter unregistered groups' option is enabled. 11. Support data driven multicast learned automatically 12. VLAN trunking 13. Loopback detection v2.0 14. Support limited IP multicast address ranges

Firmware Version	MIB File	New Features
v2.00.B27	lldp.mib, lldp-dot1.mib, lldp-dot3.mib	LLDP
	Auth.mib	Be able to force the 802.1X client to go offline
	DHCPRelay.mib	Support DHCP relay option 82 remote ID
	CableDiag.mib	Cable diagnostics
	MldSnP.mib	MLD Snooping v1 and v2 awareness
	dosprev.mib	DoS attack Prevention
	IPMacBind.mib	IP-MAC-Port Binding v3.3
	QinQ.mib	Support Port-based QinQ (TPID of outer tag can not be configured to 0x8100)
v1.00.B32	First release, please refer to datasheet and manual for detail MIB supported	

Changes of Command Line Interface:

Fireware Version	Changes
v2.00.B27	<ol style="list-style-type: none"> 1. Modify "config traffic control <portlist> dlf " to "config traffic control <portlist> unicast" 2. Remove "config traffic control_recover [<portlist> all]" 3. Modify the display "config bandwidth" to "config bandwidth_control" while show configuration file 4. Remove "legacy_pd [enable disable]" command
v1.00.B32	First release, please refer to CLI Manual for detail command line instructions

Problems Fixed:

Firmware Version	Problems Fixed
v2.00.B27	<ol style="list-style-type: none"> 1. If SIM commander switch connects to member switch via tag ports, it is unable to upload/download member's configuration (DI20071218000005) 2. If STP is enabled on ports, 'show ports' command will cause screen to freeze (DI20071224000008) 3. If STP is disabled, show ports and then reset, it will cause high CPU utilization (DI20080114000015) 4. Show port list from left to right via SNMP (DI20080116000014) 5. Config ports command lacks learning enable/disable parameter (DI20080201000009) 6. While config multicast filter, unregistered groups on all ports cannot be learned as multicast router port (DI20080214000001) 7. 802.1X authentication process with PEAP protocol takes a long time to complete (DI20080228000013) 8. Incorrect display format while execute show current config

	<p>(DI20080318000010)</p> <p>9. MAC address search issue on FDB monitor function (DI20080317000016,DI20080314000008)</p> <p>10. System interface cannot change to other VLAN while the switch is set as DHCP client (DI20080325000012)</p> <p>11. CPU high utilization while STP and LBD are enabled at the same time (DI20080331000015)</p> <p>12. Multicast client is unable to send leave packet if new VLAN is created on the switch (DI20080624000008)</p> <p>13. Filter unregistered groups on the port will block multicast control packets (DI20080421000020)</p> <p>14. IF customer uses SNMP module command and then powers off/on, switch will enter exception mode and reboot cyclically (DI20080526000007)</p> <p>15. SIM feature only works on default VLAN (DI20080604000018)</p> <p>16. While enable LACP connection, system interface cannot be accessed (DI20080404000005)</p> <p>17. Different ACL rules sequence will make ACL entries configure fail (DI20080730000018)</p> <p>18. SSH fatal error while running perl script from client (DI20080804000004)</p> <p>19. Dynamic VLAN assignment does not work if the RADIUS server is Juniper Funk Steel (DI20071130000015)</p> <p>20. While enable bandwidth control on port 25 and send packets over the rate limit from port 25 to 26, packet loss will occur from port 26 to 25 (DI20080129000025)</p>
v1.00.B32	First release

* D-Link tracking number is enclosed in ()

Known Issues:

Fireware Version	Known Issues
v2.00.B27	<ol style="list-style-type: none"> [ISM VLAN] "config igmp_snooping all state enable" will fail if ISM VLANs exist [DoS attack prevention] A PC of class A, B PC with broadcast IP address x.x.x.255, all of ping packets will be dropped, because of Smart attack prevention enable by default [Trunk] If a port enables GVRP and learned dynamic VLANs from other switches, this port cannot be configured as trunk port [MLD Snooping] MLD v1 snooping uses "Node Timeout" parameter to age out the multicast group, but MLD v2 snooping uses "Query Interval * Robustness Value + Max Response Time" to age out the multicast group [Dynamic IP Multicast Learning] The CPU utilization will be up to 100%, if there have joined the multicast group 225.0.0.0 (MAC: 01-00-5E-00-00-00) first, and learned the Date driven with multicast address 225.1.1.8 (MAC:01-00-5E-01-01-08) [Flow control] If 100M fiber port config as speed auto mode, the flow control state will always be disabled [802.1X] 802.1X authentication packets will be dropped when GVRP ingress

	<p>checking enable on the same port and the port will not belong to any VLAN member</p> <p>8. [ACL user defined packet content] User defined packet content ACL cannot block ARP request packets because there are IMPB auto recovery with high ACL priority in the background</p> <p>9. [MSTP] If adding 4K VLAN to one MSTP instance, it will takes one hour to restart the switch</p> <p>10. [QinQ] QinQ outer Tag does not support TPID 0x8100</p> <p>11. [QinQ + STP] While enable QinQ, the STP BPDU DA MAC address should be 01-80-C2-00-00-08 on NNI ports and 01-80-C2-00-00-00 on UNI ports, but the current implement of DES-3028/52 series is still use 01-80-C2-00-00-00 on both NNI and UNI ports</p>
V1.00.B32	None

Related Documentation:

- DES-3028/52 Series User Manual
- DES-3028/52 Series CLI Manual