Firmware Version: v2.60.017
Prom Code Version: v1.00.B008
Published: Jul 23, 2010

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:

Firmware Version	Date	Model	Hardware Version
Runtime: v2.60.017 Prom: v1.00.B008	23-Jul-10	DES-3528	A1, A2, A3, A4
		DES-3528DC	A1, A2
		DES-3528P	A1, A2
		DES-3552	A1, A2, A3
		DES-3552P	A1, A2
Runtime: v2.01.B042 Prom: v1.00.B008	27-Nov-09	DES-3528	A1, A2, A3, A4
		DES-3528DC	A1, A2
		DES-3528P	A1, A2
		DES-3552	A1, A2, A3
		DES-3552P	A1, A2
Runtime: v2.00.B033 Prom: v1.00.B007	08-June-09	DES-3528	A1, A2, A3, A4
		DES-3528DC	A1, A2
		DES-3528P	A1, A2
		DES-3552	A1, A2, A3
Runtime: v1.03.B013 Prom: v1.00.B007	20-Mar-09	DES-3528	A1, A2, A3, A4
		DES-3528DC	A1, A2
		DES-3528P	A1, A2
		DES-3552	A1, A2, A3
Runtime: v1.01B030 Prom: 1.00.B006	23-Apr-08	DES-3528	A1

Upgrade Instructions:

Caution: This version only supports direct firmware upgrade from v1.03 or later version. Direct upgrade from any version prior to v1.03 is not suggested and may result in unknown issues. Downgrade to any version prior to v.1.03 is not supported.
If one of the switch images has the firmware version prior to v.1.03, then this image can not be selected as the boot up image.

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 using 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> <path_filename 64> {image_id <int 1-2>}]	Download firmware file from the TFTP server to the switch.
config firmware image_id <1-2> [delete | boot_up]	Change the boot up image file.
show firmware_information	Display the information of current boot image and configuration.
reboot	Reboot the switch.

Example:

1. **DES-3528:5#download firmware_fromTFTP 10.90.90.91 R200B033.had image_id 2**

```
Command: download firmware_fromTFTP 10.90.90.91 R200B033.had image_id 2

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

2. **DES-3528:5#config firmware image_id 2 boot_up**

```
Command: config firmware image_id 2 boot_up

Success.
```

3. **DES-3528:5#show firmware information**

```
Command: show firmware information

 ID Version   Size(B)  Update Time          From                 User
 -- --------- ------- -------------------- ------------------ ---------------
1  1.03.B008 2450452 2009/02/04 17:00:26 10.90.90.91(R)      Anonymous
*2  2.00.B033 2730615 2009/08/05 02:25:85 10.90.90.91(R)      Anonymous
```

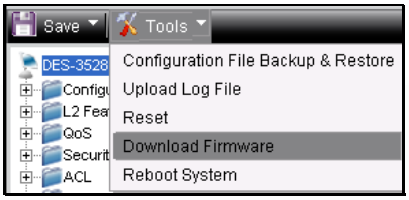
```
'*' means boot up firmware
(R) means firmware update through Serial Port(RS232)
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SSH) means firmware update through SSH
(SIM) means firmware update through Single IP Management
```

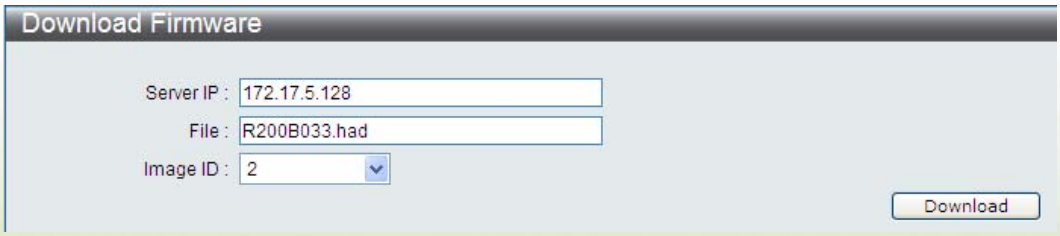
4. **DES-3528:5#reboot**

```
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.B007
--------------------------------------------------------------------------

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

  MAC Address   : 00-1E-58-4F-F7-D0
  H/W Version   : A1

  Please wait, loading V2.00.B033 Runtime image .....  100 %
  UART init .....................
  Device Discovery ..................................  100 %
  Configuration init ................................  100 %
```

Upgrade using Web-UI

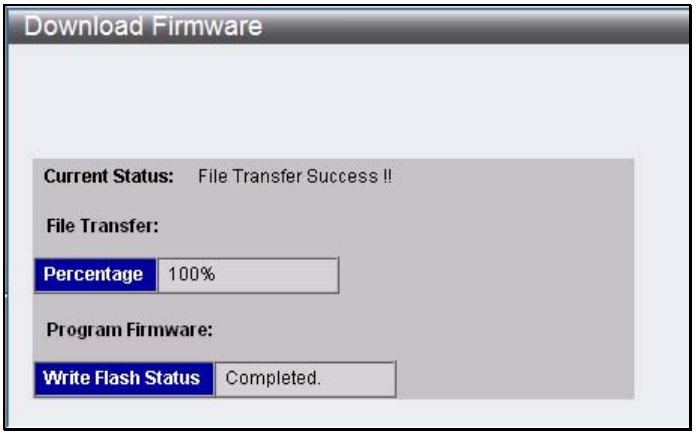
1. Connect a workstation installed with java SE runtime environment to any switch port of the device.
2. Open the web browser from the workstation and enter the IP address of the switch. The switch's default IP address is 10.90.90.90.
3. Enter administrator's username and password when prompted. It should 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. Select the Image ID you would like to store the firmware file.
8. Click "**Download**" button.
9. Wait until the "File Transfer" status reaches 100% and the "Program Firmware" status shows

"completed".



10. To select the boot up image used for next reboot, click **Configuration > Firmware information** in the function tree. Click corresponding "**Set Boot**" 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.

New Features:

Firmware Version	New Features
v2.60.017	1. JWAC enhancement: ◆ Be able to show IP address and user ID with MAC address for authenticated JWAC user in logs. ◆ Support roaming function for authenticated user between ports of the same VLAN. 2. DES-3528P and DES-3552P support legacy PoE Powered Device (PD). 3. IPv6 ready logo phase 2 host mode 4. DHCPv6 client 5. IPv6 dual stack 6. IPv6 Management via Web, SNMP and Telnet 7. WAC enhancement: ◆ Support IPv6 clients for host-based WAC ◆ Support roaming function for authenticated user between ports of the same VLAN. 8. DHCPv6 Relay 9. IPv6 Neighbor Discovery 10. Compound Authentication ◆ Any mode (802.1X, MAC, WAC, JWAC) ◆ 802.1X+IMPB, MAC+IMPB, WAC+IMPB, JWAC+IMPB 11. Add port link change trap 12. Change the aging time granularity of ARP table to 1 minute 13. 4-level user account 14. Memory utilization monitoring by SNMP, CLI & Web 15. Support Inter-VLAN routing feature: ◆ Dynamic host route ◆ IPv4/v6 static route 16. Traceroute 17. L2 Protocol Tunneling 18. Per port, per VLAN MAC address learning control 19. ERPS 20. IMPB enhancements: ◆ IMPB 3.8 ◆ DHCPv6 and NDP Snooping 21. 802.3ah extension: D-link Unidirectional Link Detection (DULD) 22. Enlarge the IGMP/MLD Snooping Group to 1024 23. Support RADIUS failover options when RADIUS times out: ◆ Use local database for authentication or ◆ Bypass authentication and assign client to port VLAN or guest VLAN or ◆ Block the client for a period of time.
v2.01.B042	1. Support new model DES-3552P
v2.00.B033	1. Cable Diagnostics 2. MDI/MDIX function manual disablement

	3. IGMP Snooping enhancement ◆ Host-Based IGMP Snooping Fast Leave ◆ IGMP v3 source filter ◆ Allow unregistered multicast traffic (not in multicast table) being forwarded to the router port even when the multicast filtering mode is set to 'filter_unregistered_groups' ◆ Support the configuration of maximum allowed multicast groups. Responsive actions inclulding drop or replacement can be triggered while the threshold is reached ◆ Support the setting of Limited IP Multicast profile on a per VLAN basis 4. MLD v2 source filter 5. Loopback detection: Support various traps for loopback detection status including loop_detected, loop_cleared and both 6. 802.3ah Ethernet OAM 7. 802.1ag CFM 8. RSPAN (Remote SPAN) 9. Time-based PoE 10. Physical Stacking Architecture 11. When under QinQ mode, the switch NNI port supports the manual selection between 802.1ad and 802.1d destination address formats for the GVRP packets flowing through it, providing better interoperability with legacy devices that only understand GVRP address in 802.1d format.
v2.00.B033	12. ISM VLAN enhancement ◆ IPv6 MLD snooping v1/v2 ◆ Source ports can be untagged ◆ Support the modification of ISM VLAN's priority level for better traffic control ◆ Support the configuration of two ISM VLAN source ports on the switch. When working with STP , it will allow the forwarding of multicast stream using backup link in case the primary link goes down 13. Advanced QinQ functions that allow the insertion of customer VLAN tag and the configuration of inner TPID 14. Voice VLAN 15. Subnet-based VLAN 16. VLAN trunking 17. ARP entry's minimum aging time can be set to 30 sec. ARP entry's aging time can remain unaffected when being accessed by switch's internal process 18. Support 16 IP interfaces 19. Policy-based routing 20. Proxy ARP 21. SNMP trap and system log support for Gratuitous ARP events 22. Configurable user 802.1p priority on each port. 23. Scheduling mechanisms (strict or WRR) can be configured on a per port basis. 24. CoS Bandwidth Control that supports ◆ Per egress queue bandwidth control ◆ Per egress queue bandwidth guarantee 25. ACL function supports up to 14 profiles and 1792 rules per system 26. VLAN-based ACL 27. Allows the configuration of SSH port to any desired port number 28. Broadcast/Multicast Storm Control allows the configuration of 5 minutes recovery timer for shutdown ports

v2.00.B033	29. IMPB V3.5 ◆ Configurable threshold number for illegitimate entries that can be recorded in the FDB 30. Web-based Access Control (WAC) enhancement ◆ Host-based authentication ◆ Dynamic VLAN assignment based on the VLAN attribute dispatched from RADIUS server after successful authentication with RADIUS ◆ Identity-driven QoS: Support the assignment of 1. Ingress/egress bandwidth attributes 2. 802.1p priority attribute - to the port based on the attributes dispatched from RADIUS server after successful authentication with RADIUS 31. MAC-based Access Control (MAC) enhancement ◆ Port-based Authentication ◆ Identity-driven QoS: Support the assignment of 1. Ingress/egress bandwidth attributes 2. 802.1p priority attribute - to the port based on the attributes dispatched from RADIUS server after successful authentication with RADIUS ◆ Host-based Authentication: enlarge the number of supported users from 16 per port, 448 per switch, to 1000 per port, switch and stack. ◆ Host-based Authentication supports the manual configuration of host numbers from 1 to 1000 on a per port basis 32. 802.1X ◆ Identity-driven QoS: Support the assignment of 1. Ingress/egress bandwidth attributes 2. 802.1p priority attribute - to the port based on the attributes dispatched from RADIUS server after successful authentication with RADIUS ◆ Host-based Access Control: enlarge the number of supported users from 16 per port, 448 per switch, to 448 per port, switch and stack. ◆ Support “Reply Message” attribute from RADIUS server so the switch can forward the “Reply Message” attribute to 802.1x clients 33. Japanese Web-based Access Control (JWAC): Enhance the maximum number of on-line users from 256 per port/switch to 1000 per port/switch/stack 34. MAC filtering via FDB 35. L3 Control Packet Filtering: Support the filtering of DVMRP, PIM, IGMP Query, OSPF, RIP, or VRRP packets. 36. Multiple Authentication 37. Authentication database failover: Be able to switch to local database for authentication when RADIUS server fails. 38. Remove the display of MAC address information from "show log" switch command 39. Telnet Client 40. Trusted host that supports up to 10 IP addresses or subnet entries in total 41. SYSLOG ◆ Support WAC/MAC event logging ◆ Support storm control block mode logging ◆ Support spoofing attack logging with IP, MAC address and corresponding port information 42. sFlow support 43. DHCP relay option 60, 61 44. DHCP relay option 82 with group ID support 45. DHCP Server enhancement: Support DHCP server configuration via Web GUI & SNMP 46. Add user IP information in admin ID/password change event logging 47. DNS Relay

v2.00.B033	48. Send trap and log when the switch temperature goes over 80 Degrees or downs under 75 Degrees 49. ARP Spoofing Attack Prevention 50. Show product serial number on Web GUI and CLI 51. Add BPDU Attack Protection supports in WEB and MIB 52. When using SNMP to command the switch to download a firmware file, send a trap while the firmware upgrade finishes
v1.03.B013	1. Support DES-3528DC, DES-3528P, DES-3552 2. DHCP Local Relay 3. PPPoE Circuit-ID Tag Insertion 4. DHCP Server (Only supports CLI. No Web GUI & SNMP) 5. BPDU Attack Protection (Only supports CLI. No Web GUI & SNMP) 6. Flash memory re-layout: allocate larger memory size for firmware images, allowing more features to be added in future releases. When upgrading to v1.03, new PROM code (v1.00.B007) that supports this will be installed to the switch automatically.
v1.01.B035	1. Support DES-3528 A2 hardware. 2. Support D-view 6.0 platform.
v1.01.B030	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
v2.60.017	ACL.mib	Be able to configure ACL rule and profile at the same time.
	Auth.mib	Add VLAN-based authentication feature
	L2ProtocolTunnel.mib	Support L2 Protocol Tunneling function
	DHCPRelay.mib	Use swDHCPRelayVlanCtrlTable instead of swDHCPLocalRelayMgmt to support the relay server configuration per VLAN basis.
	DULD.mib	Support DULD function
	IPMacBind.mib	1. Add IPv6 DHCP Snooping function. 2. Add IPv6 IP-MAC-Port Binding function. 3. Add ND snooping function. 4. Add IPv6 IP-MAC-Port Binding unauthenticated trap.
	Jwac.mib	Add JWAC roaming function.
	l3mgmtDES3528.mib l3mgmtDES3528dc.mib l3mgmtDES3528p.mib l3mgmtDES3552.mib l3mgmtDES3552P.mib	Add IPv4 v6 inter-VLAN routing functions
	mba.mib	1. Add MAC per VLAN authentication display function. 2. Add MAC timer setting function.
	McastFilter.mib	Add IPv6 multicast filter support
	McastVLAN.mib	Add the state configuration of multicast VLAN forward unmatched packet
	PktStormCtrl.mib	Add storm control log and recover timer
	PoE.mib	Support legacy PD detection
	ProtocolVLAN.mib	Remove swProtocolVLANTable support. Use standard MIB RFC4363 to cover this function.
	SSH.mib	Add IPv6 host address support
	StaticFdb.mib	Support static FDB configurations
	staticMacBasedVlan.mib	Be able to display the type of VLAN which belongs to compound authentication.
	SysLog.mib	Add IPv6 log server support
	VoiceVLAN.mib	Remove Voice VLAN trap support
	wac.mib	Add WAC IPv6 authentication and per VLAN authentication functions.
	erps.mib	Support ERPS function
	PortSecurity.mib	Support Port Security function
	IPv6StaticRoute.mib	Support IPv6 static route function
	vlancounter.mib	Support VLAN counter function
	ie8023ad.mib	Replace original proprietary MIB by using standard MIB
	rfc2863.mib	Support port link change trap

v2.60.017	rfc2925t.mib	Support trace route function
	rfc4022.mib	Support TCP MIB
	rfc4293.mib	Support IP forwarding table
v2.01.B042	L2mgmtDES3552P.mib L3mgmtDES3552P.mib	Support new model DES-3552P
	1. Release new D-View Module for DES-3552P 2. Release new D-View Module for DES-3528/28DC/28P/52 to support stacking with DES-3552P	
v2.00.B033	ACL.mib	1. Support VLAN-based ACL 2. Support IPv6-based ACL for TCP/UDP protocols 3. Support up to 14 ACL profiles and 1792 ACL rules per system
	ARPSpoofingPrevention.mib	Support ARP Spoofing Attack Prevention feature
	Auth.mib	1. Support the display of 802.1X Host-based Access Control entries 2. Support Authentication Database Failover feature 3. Support RADIUS Authorization feature that accepts the assignment of VLAN and QoS values dispatched from RADIUS server after successful authentication with RADIUS
	BPDUProtection.mib	Add BPDU Attack Protection supports in WEB and MIB
	CableDiag.mib	Support Cable Diagnostics feature
	DHCPRelay.mib	1. Support DHCP relay option 82 with group ID feature 2. Support DHCP relay option 60, 61
	DHCPServer.mib	Support DHCP Server feature
	Equipment.mib	Support the sending of trap and log when the switch temperature goes over 80 Degrees or downs under 75 Degrees
	Filtering.mib	Support L3 Control Packet Filtering feature
	Genmgmt.mib	1. Support SNMP trap notification when failing to access flash file system 2. When using SNMP to command the switch to download a firmware file, send a trap while the firmware upgrade finishes
	IPMacBind.mib	Support IMPB v3.5 configurable threshold number for illegitimate entries that can be recorded in the FDB
	Jwac.mib	1. Support JWAC update server state 2. Support Authentication Database Failover feature 3. Support RADIUS Authorization feature that accepts the assignment of VLAN and QoS values dispatched from RADIUS server after successful authentication with RADIUS
	Jwac.mib	Support Local Authorization feature that accepts the assignment of VLAN value from local database after successful authentication with local database

v2.00.B033	l2mgmtDES3528.mib, l2mgmtDES3528dc.mib, l2mgmtDES3528p.mib, l2mgmtDES3552.mib	When under QinQ mode, the switch NNI port supports the manual selection between 802.1ad and 802.1d destination address formats for the GVRP packets flowing through it.
	l2mgmtDES3528.mib, l2mgmtDES3528dc.mib, l2mgmtDES3528p.mib, l2mgmtDES3552.mib, ie8021ag.mib	1. Support 802.1ag CFM feature 2. Support DHCP Local relay feature 3. Support VLAN Trunking feature
	L3mgmtDES3528.mib, L3mgmtDES3528dc.mib, L3mgmtDES3528p.mib, L3mgmtDES3552.mib	1. Support the setting of ARP entry's minimum aging time to 30 sec. ARP entry's aging time can remain unaffected when being accessed by switch's internal process 2. Support DNS relay feature
	mba.mib	1. Support configurable aging time, hold-down time and port-based access control for MAC-based Access Control (MAC) 2. Support Authentication Database Failover feature for MAC 3. Support RADIUS Authorization feature that accepts the assignment of VLAN and QoS values dispatched from RADIUS server after successful authentication with RADIUS 4. Support Local Authorization feature that accepts the assignment of VLAN value from local database after successful authentication with local database
	McastFilter.mib	1. Support the configuration of maximum allowed multicast groups (IPv4 only) 2. Support Limited IP Multicast profile per VLAN (IPv4 only)
	McastSnooping.mib; McastVLAN.mib	Use McastSnooping.mib and McastVLAN.mib to replace the multicast features from L2mgmt.mib
	PoE.mib	Support Time-based PoE feature
	QinQ.mib	Support advanced QinQ functions that allow the insertion of customer VLAN tag and the configuration of inner TPID
	Qos.mib	1. Support configurable default 802.1p priority on each port. 2. Scheduling mechanisms (strict or WRR) can be configured on a per port basis. (QoS related features have been removed from L2mgmt.mib)
	RSPAN.mib	Support RSPAN feature
	sFlow.mib	Support sFlow feature
	SSH.mib	Support the configuration of SSH port to any desired port number
	SubnetVLAN.mib	Support subnet-based VLAN feature
	VoiceVLAN.mib	Support Voice VLAN feature

v2.00.B033	WAC.mib	1. Support port-based access control for WAC 2. Support Authentication Database Failover feature for WAC 3. Support RADIUS Authorization feature that accepts the assignment of VLAN and QoS values dispatched from RADIUS server after successful authentication with RADIUS 4. Support Local Authorization feature that accepts the assignment of VLAN value from local database after successful authentication with local database
	MSTP.mib	Add MSTP conformance to IEEE 802.1Q-2005 standard
	HCNUM-TC.mib; RFC 1850.mib	Add HCNUM-TC.mib and RFC 1850.mib for loading L3mgmt.mib
	ie8023ah.mib	Support 802.3ah OAM feature
	RFC4188.mib	Use RFC4188.mib to replace RFC1493.mib
v1.03.B013	IPMacBind.mib	1. Modify the variable binding of the trap of IP-MAC-Port Binding 2. Modify the value of swIpMacBindingACLMode: "enable" to "enabled", "disable" to "disabled".
	l2mgmtDES3528.mib l2mgmtDES3528dc.mib l2mgmtDES3528p.mib l2mgmtDES3552.mib	1. Support DHCP Local Relay 2. Support PPPoE Circuit-ID Tag Insertion
v1.01.B035	None	
v1.01.B030	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.
The switch will transfer the old commands in configuration files automatically to new style when applying the configuration files as running configuration. If there are old parameters which exceed the range of the new command, switch will use default value instead.

Firmware Version	Changes
v2.60.017	1. config stacking mode changes to config stacking_mode 2. config bpdu_protection ports … mode [drop | block | disable]} changes to config bpdu_protection ports … mode [drop | block | shutdown]} 3. download [firmware_fromTFTP … <path_filename 64> … <path_filename 64> …] changes to download [firmware_fromTFTP … src_file <path_filename 64> … src_file <path_filename 64> …] **Note:** From v2.60 onward, the src_file parameter is added. This improvement is to avoid potential command parsing problem. If you have upgraded the firmware to v2.60 or onward, and are using script to manipulate firmware or config file, please do not forget to add this parameter to the script. 4. delete igmp_snooping multicast_vlan_group_profile [<profile_name 1-32> |all] changes to delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> |all] 5. delete mld_snooping multicast_vlan_group_profile [<profile_name 1-32> |all] changes to delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> |all] 6. config voice_vlan trap_log [enable|disable] changes to config voice_vlan log state[enable|disable] 7. show local_route [ipv4|ipv6] changes to show local_route 8. config traffic control … time_interval <value 5-30>} changes to config traffic control … time_interval <sec 5-600>} 9. config mac_based_access_control ports [<portlist> | all] { state [enable | disable]| mode [port_based | host_based]| aging_time [infinite | <min1-1440>] | block_time [infinite | <sec 1-300>] | max_users [<value 1-1000> | no_limit]}(1) changes to

	config mac_based_access_control ports [<portlist> | all] { state [enable | disable]| aging_time [infinite|<min 1-1440>]| block_time <sec 0-300> |max_users [<value 1-1000> | no_limit]}(1)
v2.60.017	10. config jwac ports … block_time [<sec 0-300>] | auth_mode [host based | port_based]} changes to config jwac ports … block_time [<sec 0-300>]} 11. Remove following command config wac auth_failover [enable | disable] config wac authorization network {radius [enable | disable] | local [enable | disable]} config jwac auth_failover [enable | disable] config 802.1x auth_mode [port_based | mac_based] config 802.1x auth_failover [enable | disable] config 802.1x authorization network radius [enable | disable] enable authorization network enable authorization attributes
v2.01.B042	None
v2.00.B033	1. Change the command “config dhcp pool dns_server_address ” to “config dhcp pool dns_server” 2. Change the command “show dhcp_binding ” to “show dhcp binding ” 3. Change the command “clear dhcp_binding ” to “clear dhcp binding ” 4. Change the command “delete jwac host” to “clear jwac auth_state” 5. Change the command “Show jwac host” to “show jwac auth_state ports” 6. Change the command “show mac_based_access_control auth_mac ” to “show mac_based_access_control auth_state ports” 7. Change the command “delete jwac host” to “clear jwac auth_state” 8. Change the command “Show jwac host” to “show jwac auth_state ports” 9. Change the command “config igmp_snooping vlan" to “config igmp_snooping“ with following parameter changes: ◆ Remove parameters: <vlan_name 32> | all] {host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state [enable | disable]} ◆ Add Paramteres: <vlan_name 32> | vlanid <vlanid_list> | all] { state [enable|disable] | fast_leave [enable|disable] | report_suppression [enable | disable]} 10. Modify “config igmp_snooping multicast_vlan_group" command's parameters: ◆ Remove parameters: <vlan_name 32> [add <mcast_address_list> | delete [<mcast_address_list> | delete_all]] ◆ Add Paramteres: <vlan_name 32> [add | delete] profile_name< profile_name 1-32>] 11. Modify “config max_mcast_group" command’s parameters ◆ Remove parameters: <portlist> max_group [<value 1-256> | infinite] ◆ Add Paramteres: <portlist>|vlanid <vidlist>] {max_group [<value 1-1024>|infinite]| action [drop | replace]}

v1.03.B013	None
v1.01.B035	None
v1.01.B030	First release

Problem Fixed:

Firmware Version	Problems Fixed
v2.60.017	1. DHCPv6 packet cannot be filtered by ACL. 2. When relaying the DHCP request across two or more DES-3528/52, and all these switches are enabled with DHCP relay, clients cannot get the IP correctly. (DRU20100402000005) 3. The status of MAC address in FDB will be changed from Permanent to UnBlockByMBA after the host is authenticated by MAC. While it shouldn't be changed. 4. Switch may get into exception mode when running over 5 hours with JWAC concurrent users always over 120. (DI20091005000014) 5. Sometimes the status of authenticated JWAC clients will be back to "JWAC_Authing" if the clients are some particular HP models with Vista OS. (DI20100324000007) 6. Port list information cannot be saved in configuration file for the command: "config address_binding ip_mac ports <portlist> state enable ipv6" (DRU20100526000002) 7. The drop packet counter will increase when receiving ICMPv6 packet. 8. Configuration cannot be saved via Web UI when using Linux + Firefox 3.5.9. (DRU20100519000002) 9. When 802.3x flow control is enabled, the switch does not count dropped packets. (DUSA20100622000001) 10. It is required to create an account 'enable' when using the command "enable admin". (DEUR20100705000008)
v2.01.B042	1. IMPB ARP mode can not be set properly by D-View 6.0 with E2ES plug-in and there is no warning message returning to D-View 6 (DT20090604000001) 2. Sometimes the switch can not be reset or the config can not be downloaded via WEB UI (DI20091029000008)(DI20091102000017) 3. When backup master taking over the job of stacking master, the LACP channel's MAC address changes to the backup master's address and LACP takes 5~7 seconds to recover. (DI20090818000003) 4. When creating two LACP groups and making the port of the LACP group ID 2 link down, the system interface goes down. (DI20090828000019) 5. After manipulating VLAN settings and then resetting the switch configuration, the system interface goes down and pops up invalid messages. (DI20090901000003) 6. When jwac udp_filtering is disabled, DHCP packets still can not pass through the switch. (DI20090731000013) 7. When enabling LBD function and MAC-based Access Control with RADIUS at the same time, LBD will fail. (DI20090728000008) 8. JWAC function will fail if client comes from tagged port. (DI20090710000006) 9. QinQ and ISM-VLAN are not designed to be activated at the same time. However they can be enabled at the same time. (DI20090529000010) 10. When using a particular command to create ACL, the switch will pop up the message "The profile name already exist.". but this profile name actually does not exist. 11. All packets to the management interface was counted as 'dropped' (DI20090625000019)2 OIDs for port security function do not allowed to be set simultaneously, which causes the following command failed: snmpset -c private -v 2c 10.77.0.126 1.3.6.1.2.1.17.7.1.3.1.1.3.141.0.0.0.0.0.22.0 x 8000000000000000 && snmpset -c private -v 2c 10.77.0.126 1.3.6.1.2.1.17.7.1.3.1.1.4.141.0.0.0.0.0.22.0 i 3 12. The switch cannot reply to the SNMP get request for "ifNumber:0" correctly.

v2.01.B042	13. Client can not get IP via the switch's DHCP relay function if the client resides on a VLAN that does not have an IP interface and system interface does not link up (DI20090427000014) 14. Default gateway configuration loses after switch rebooting. (DI20090713000009)
v2.00.B033	1. The switch will enter exception mode when opening a SSH login session to the switch using Open SSH 5.1. (DI20090317000025) 2. The switch doesn't support the automatic assignment of ACL ID when users want to create an ACL rule through SNMP. (DI20090318000013) 3. The switch's auto configuration function will fail when DHCP and TFTP servers are located on different computer devices.(DI20090331000006) 4. In a Spanning-tree enabled network environment, no matter which switch port goes down and results in the STP topology change, the generated log message always indicates that the change comes from switch port1 as "Topology changed (Instance:0, port:1)".(DI20090403000010) 5. The switch does not log user out even when "Idle Time" is set in JWAC function (i.e. one minute) and the user session has been idled for more than the specified idle time.(DI20090409000007)
v1.03.B013	1. When the maximum number of DHCP snooping entries is configured, and the status of a DHCP snooping entry changes from 'inactive' to 'active' (eg. The corresponding port becomes link-up again), this entry will not be confined by the configured maximum number. (DI20081028000003) 2. If a WAC client's IP address belongs to the trusted host list, WAC authentication window does not pop up on that client. (DT20081114000001) 3. The ISM-VLAN function does not forward multicast traffic to a client if this client sends the IGMP V3 membership report to join the multicast group. (DEUR20081105000004) 4. When Q-in-Q is not applied on Management VLAN, but other VLANs, traffic from Management VLAN will be double tagged at NNI port. (DI20081208000010) 5. The switch will enter exception mode if a client tries to do WAC authentication and executes MSN 8.5 to login in the same time. (DT20081201000001) 6. The switch does not display SIM topology correctly on FireFox 3.01 and JAVA 1.60_11B03. (DI20081218000018) 7. The switch can not be managed by SIM when DES-3528 acts as the SIM member and DES-3526 as the SIM commander. (DI20081121000011) 8. When a client connects to the switch, uses FTP to download data via PPPoE connection, the FTP session disconnects after running for 1 ~ 2 minutes. (DI20090111000004)
v1.01.B035	1. The Bandwidth Control and ACL Flow Meter (flow-based bandwidth control) are inaccurate at the 1st second of traffic transmission. The allowed traffic bandwidth is around double times to the configured value. (Known Issue of 1.01.B030)
v1.01.B030	First release

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues	Workaround
V2.60.017	1. By default, R2.60 supports only 12 ACL profile and 1536 rules which is less than R2.01 (14 profiles, 1792 rules). Some ACL setting in previous configuration file may lose after firmware upgrade.	1. Disable inter-VLAN routing feature to gain full 14 ACL profiles and 1792 rules support. 2. Make sure the current ACL profile is under 12 when re-activating the inter-VLAN routing function.
	2. The firmware version in boot up page will show "v2.60..017"	None
v2.01.B042	None	None
v2.00.B033	1. The web interface does not support user logout and automatic logout when using Apple's Safari web browser.	None
	2. The web interface will generate error message when configuring CFM loopback function through it. However it is working fine when configuring using CLI.	Upgrade to v2.60.017 or above.
v1.03.B013	1. Per port mapping of 802.1p priority and class is not supported when packets flowing between block 1 (port 1~24/51/52) and block 2 (port 25~50), and across devices in the same physical stack. When this happens the switch will use default mapping instead of the configured class mapping. 2. Flow control is not supported for packets flowing between block 1 (port 1~24/51/52) and block 2 (port 25~50), and across devices in the same physical stack. 3. Traffic flowing between block 1 and block 2 does not reach line rate (max. 5% packet loss) when the packet size is between 64~97 bytes. 4. The CPU handles control signals and the utilization will be 11~13% with default settings. 5. When mirroring egress untagged packets in line speed, the mirrored packets can not reach line speed.	None
v1.01.B035	None	None
v1.01.B030	The Bandwidth Control and ACL Flow Meter (flow-based bandwidth control) are inaccurate at the 1st second of traffic transmission. The allowed traffic bandwidth is around double times to the configured value. Starting from 2nd second the allowed bandwidth becomes normal.	Upgrade to v1.01.B035 or above.

Related Documentation:

- DES-3528/52 Series User Manual
- DES-3528/52 Series CLI Manual