



Firmware Version: V4.04.004
Prom Code Version: V4.00.002
Published: Jan/21, 2013

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	5
DES-3200 series C1: Upgrade using CLI (serial port)	5
Upgrade using Web-UI:	6
DES-3200 A1/B1 : Upgrade using CLI (serial port)	9
Upgrade using Web-UI	10
New Features:	13
Changes of MIB & D-View Module:	14
Changes of Command Line Interface:	15
Problem Fixed:	17
Known Issues:	20
Related Documentation:	27

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
Runtime: v.4.04.004 Prom: v4.00.002	Jan-15-13	DES-3200-10	C1
		DES-3200-10-DC	C1
		DES-3200-18	C1
		DES-3200-18-DC	C1
		DES-3200-26	C1
		DES-3200-26-DC	C1
		DES-3200-28	C1
		DES-3200-28/ME	C1
		DES-3200-28F	C1
		DES-3200-28P	C1
		DES-3200-52	C1
		DES-3200-52-DC	C1
		DES-3200-52P	C1
Runtime: v.4.03.004 Prom: v4.00.002	Oct-17-12	DES-3200-10	C1
		DES-3200-10-DC	C1
		DES-3200-18	C1
		DES-3200-18-DC	C1
		DES-3200-26	C1
		DES-3200-26-DC	C1
		DES-3200-28	C1
		DES-3200-28F	C1
		DES-3200-28P	C1
		DES-3200-52	C1
		DES-3200-52-DC	C1

		DES-3200-52P	C1
Runtime: v.4.02.004 Prom: v4.00.002	30-Apr-12	DES-3200-10	C1
		DES-3200-10-DC	C1
		DES-3200-26	C1
		DES-3200-26-DC	C1
		DES-3200-28	C1
		DES-3200-28P	C1
		DES-3200-52	C1
		DES-3200-52P	C1
Runtime: v.4.00.024 Prom: v4.00.002	10-Jan-12	DES-3200-26	C1
		DES-3200-28	C1
		DES-3200-28P	C1
		DES-3200-52	C1
		DES-3200-52P	C1
Runtime: v.4.00.020 Prom: v4.00.001	6-Dec-11	DES-3200-28P	C1
		DES-3200-52	C1
		DES-3200-52P	C1
Runtime: v1.28.009 Prom: v1.00.007	13-Jun-11	DES-3200-10	A1
		DES-3200-18	A1
		DES-3200-26	A1
		DES-3200-28	A1
		DES-3200-28F	A1
		DES-3200-28/ME	A1
		DES-3200-10	B1
		DES-3200-18	B1
		DES-3200-26	B1

		DES-3200-28	B1
Runtime: v1.21.B006 Prom: v1.00.B004	11-Apr-10	DES-3200-10	A1
		DES-3200-18	A1
		DES-3200-26	A1
		DES-3200-28	A1
		DES-3200-28F	A1
Runtime: v1.0.B015 Prom: v1.00.B003	22-Oct-09	DES-3200-10	A1
		DES-3200-18	A1
		DES-3200-28	A1
		DES-3200-28F	A1

Note1: Prom v1.00.B004 adds the booting identification of DES-3200-26 device. Please do not upgrade the mentioned device (DES-3200-26) with other PROM versions

Note2: Prom v1.00.005 adds the booting identification of DES-3200-28/ME device. Please do not upgrade the mentioned device (DES-3200-28/ME) with other PROM versions

Note3: DES-3200-28/ME is specific for Russia regional project, not a WW model.

Note4: Prom v1.00.007 adds the booting identification of DES-3200-10/18/26/28 B1 device. I Please do not upgrade the mentioned device (DES-3200-10/18/26/28 B1) with other PROM versions

Note5: The Runtime code v4.00.020 & Prom v4.00.001 are for DES-3200 C1 only (DES-3200-28P/52/52P C1).

Note6: The Runtime code v4.00.024 & Prom v4.00.002 are for DES-3200 C1 only (DES-3200-26/28/28P/52/52P C1).

Note7: The Runtime code v4.02.004 & Prom v4.00.002 are for DES-3200 C1 only (DES-3200-10/10-DC/26/26-DC/28/28P/52/52P C1).

Note8: The Runtime code v4.03.004 & Prom v4.00.002 are for DES-3200 C1 only (DES-3200-10/10-DC/18/18-DC/26/26-DC/28/28F/28P/52/52-DC/52P C1).

Note9 The Runtime code v4.04.004 & Prom v4.00.002 are for DES-3200 C1 only (DES-3200-10/10-DC/18/18-DC/26/26-DC/28/28F/28/28/ME/28P/52-DC/52P C1).

Upgrade Instructions

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.

DES-3200 series C1: Upgrade using CLI (serial port)

DES-3200-10/10-DC/18/18-DC/26/26-DC/28/28F/28P/28/ME/52/52-DC/52P C1, FW: R4.04.004 or above

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> src_file <path_filename 64>}]	Download firmware file from the TFTP server to the switch.
config firmware image <path_filename64>boot_up	Change the boot up image file.
show switch	Display Switch information.
reboot	Reboot the switch.

Example:

1. **DES-3200-28P:4#download firmware_fromTFTP 10.54.71.1 src_file_DES3200_RUNTIME_V4.04.004.had**
 Command: download firmware_fromTFTP 10.54.71.1 src_file DES3200_RUNTIME_V4.04.004.had

 Connecting to server..... Done.
 Download firmware..... Done. Do not power off!
 Please wait, programming flash..... Done.
2. **DES-3200-28P:admin#config firmware image c:/DES3200_RUNTIME_V4.04.004.had boot_up**
 Command: config firmware image c:/DES3200_RUNTIME_V4.04.004.had boot_up

 Success.
3. **DES-3200-28P:4#show switch**
 Command: display the Switch information

```
DES-3200-28P:admin#show switch
Command: show switch

Device Type           : DES-3200-28P Fast Ethernet Switch
MAC Address           : 00-01-02-03-04-00
IP Address             : 10.90.90.90 (Manual)
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
Boot PROM Version     : Build 4.00.002
Firmware Version      : Build 4.04.004
Hardware Version       : C1
System Name            :
System Location        :
System Uptime         : 0 days, 2 hours, 2 minutes, 28 seconds
System Contact        :
Spanning Tree          : Disabled
GVRP                   : Disabled
IGMP Snooping         : Disabled
MLD Snooping          : Disabled
VLAN Trunk             : Disabled
Telnet                 : Enabled (TCP 23)
Web                    : Enabled (TCP 80)
SNMP                   : Enabled
SSL Status             : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

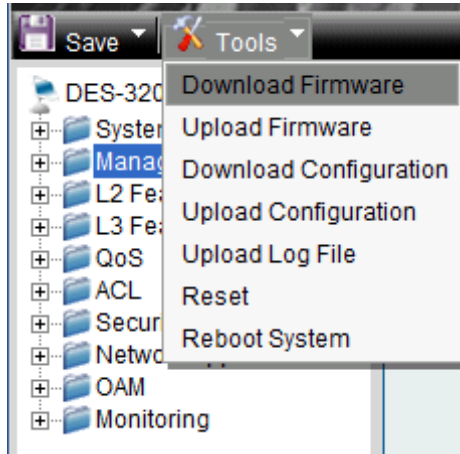
4. DES-3200-28P:admin#reboot

Command: reboot

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

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.



Download Firmware Safeguard

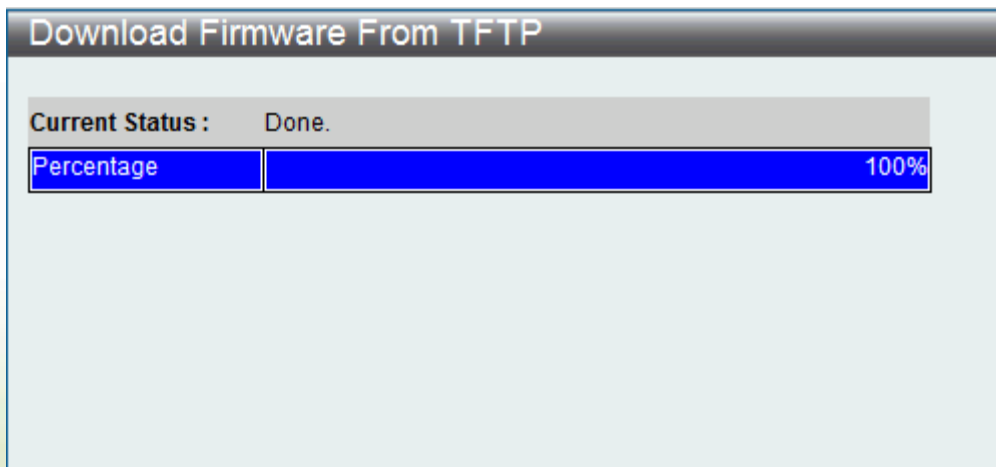
Download Firmware From TFTP
 Download Firmware From FTP
 Download Firmware From HTTP

TFTP Server IP : IPv4

Source File :

Destination File :

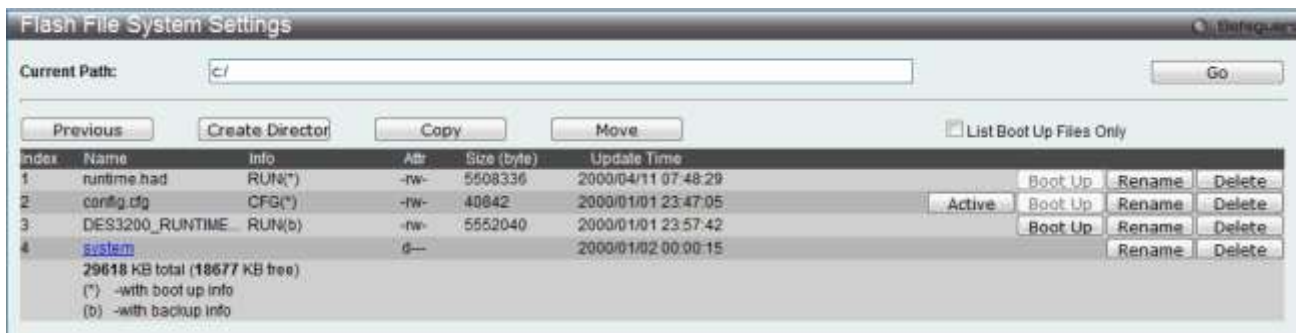
5. Enter the TFTP Server IP address.
6. Enter the location and name of the Source File on the TFTP server(ex. DES3200_RUNTIME_V4.04.004.had)
7. Click "**Download**" button.
8. Wait until the "Current Status" reaches 100% and shows "Done".



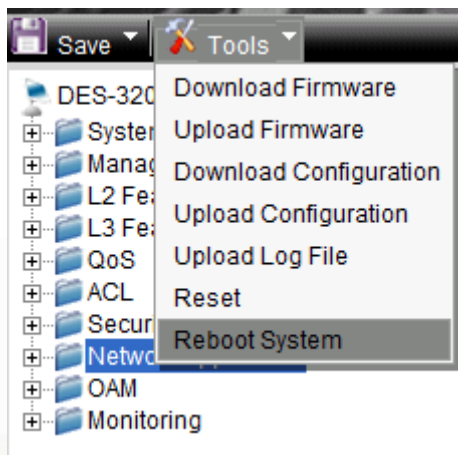
- To select the boot up image used for next reboot, click "**Network Application**" > "**Flash File System Settings**" in the function tree. Enter the Current Path string and click the Go button or click the C: to enter "Flash File System Setting- Search for Drive" window.



- Click corresponding "**Boot UP**" button to specify the firmware that will be used for next and subsequent boot up.



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



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

DES-3200 A1/B1 : Upgrade using CLI (serial port)

DES-3200-10/18/16/28/28F/28/ME A1, DES-3200-10/18/26/28 B1, FW: R1.28 or above

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: **9600**
- ◆ 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:

5. **DES-3200-28F:4#download firmware_fromTFTP 10.90.90.100 des3200_runtime_v1.21.b006.had image_id 2**
 Command: download firmware_fromTFTP 10.90.90.100 des3200_runtime_v1.20.b011.had image_id 2

 Connecting to server..... Done.
 Download firmware..... Done. Do not power off!
 Please wait, programming flash..... Done.
6. **DES-3200-28F:4#config firmware image_id 2 boot_up**
 Command: config firmware image_id 2 boot_up

 Success.
7. **DES-3200-28F:4#show firmware information**
 Command: show firmware information

ID	Version	Size(B)	Update Time	From	User
1	1.10.B014	3507464	0000/00/00 00:00:00	Serial Port (PROM)	Unknown
*2	1.21.B006	3659420	0000/00/00 00:00:00	10.90.90.100 (CONSOLE)	Anonymous

 '*'
 (SSH) : Firmware update through SSH
 (WEB) : Firmware update through WEB
 (SIM) : Firmware update through Single IP Management

(SNMP) : Firmware update through SNMP
(TELNET) : Firmware update through TELNET
(CONSOLE) : Firmware update through CONSOLE

8. **DES-3200-28F:4#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.B003

Power On Self Test 100 %

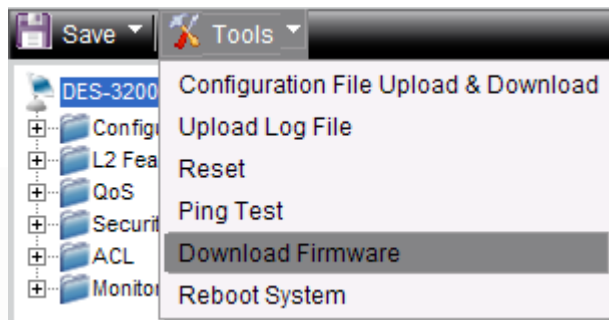
MAC Address : 00-1E-58-6E-A5-60

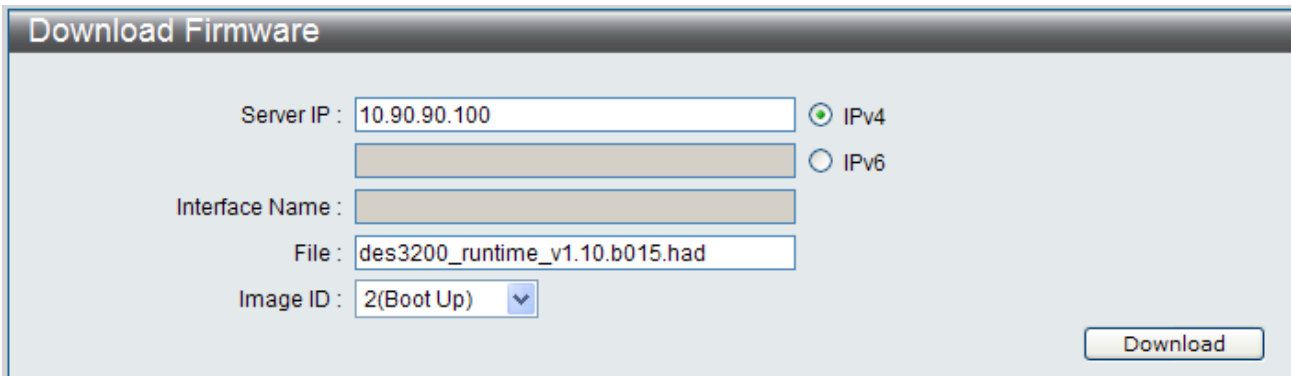
H/W Version : A1

Please wait, loading V1.20.B011 Runtime image 100 %

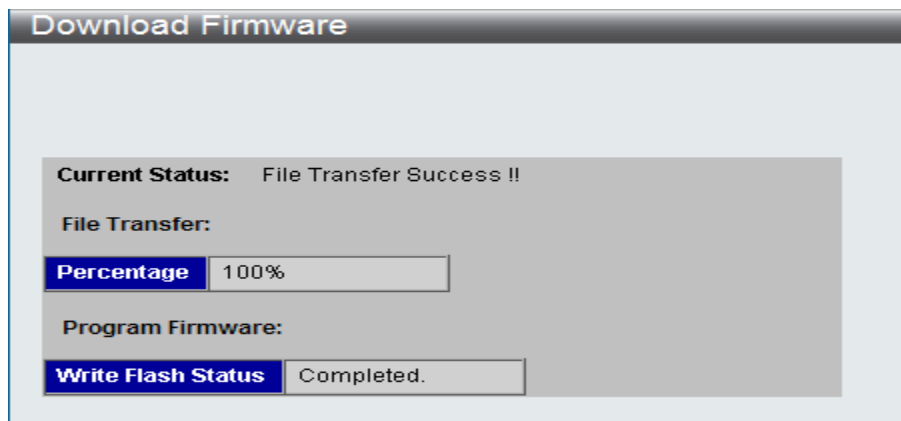
Upgrade using Web-UI:

13. Connect a workstation installed with java SE runtime environment to any switch port of the device.
14. 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.
15. Enter administrator's username and password when prompted. It should be noted that the username and password are blank by default.
16. To update switch's firmware or configuration file, select **Tools > Download Firmware** from the banner.





17. Enter the TFTP Server IP address.
18. Enter the name of the firmware file located on the TFTP server.
19. Select the Image ID you would like to store the firmware file.
20. Click "**Download**" button.
21. Wait until the "File Transfer" status reaches 100% and the "Program Firmware" status shows "completed".



22. To select the boot up image used for next reboot, click **Configuration > Firmware information** in the function tree. Click corresponding "**Boot UP**" button to specify the firmware that will be used for next and subsequent boot up.



23. To reboot the switch, select **Tools > Reboot System** from the banner.
24. Select "**Yes**" and click "**Reboot**" button to reboot the switch.

New Features:

Firmware Version (DES-3200 C1)	New Features
V4.04.004	<ol style="list-style-type: none"> 1. Support new model DES-3200-28/ME 2. Added External PSU detection and External Alarm features.
V4.03.004	<ol style="list-style-type: none"> 1. Support new models DES-3200-18/18-DC/28F/52-DC C1
V4.02.004	<ol style="list-style-type: none"> 1. Support new models DES-3200-10/10-DC/26-DC C1
V4.00.024	<ol style="list-style-type: none"> 1. Support new models DES-3200-26/28 C1
V4.00.020	<ol style="list-style-type: none"> 1. Support new models DES-3200-28P/52/52P C1

Firmware Version (DES-3200 A1/B1)	New Features
V1.28.009	<ol style="list-style-type: none"> 1. Support new models DES-3200-10/18/26/28 B1
V1.25.007	<ol style="list-style-type: none"> 1. Support new model DES-3200-28/ME 2. External alarm (ONLY in DES-3200-28/ME) 3. Redundant Power Supply (ONLY in DES-3200-28/ME)
V1.21.B006	<ol style="list-style-type: none"> 1. Support new model DES-3200-26 2. Loopback detection V4.0: Support VLAN-based detection /shutdown 3. BPDU Attack Protection 4. MAC-based Access Control (MAC): ACL assignment after successful authentication 5. Network Load Balancing (NLB) 6. 802.3ah Ethernet Link OAM 7. 802.1ag Connectivity Fault Management (CFM) 8. Ethernet Ring Protection Switching(ERPS) 9. PPPoE Circuit ID Insertion 10. MSTP instances extend to 8 11. Display uptime in command show_switch 12. Per egress queue bandwidth control 13. DHCP option 12 14. DHCP Server Screening 15. Enlarge command prompt to 32 bytes
V1.10.B015	First Release, please refer to datasheet for feature detail.

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 (DES-3200 C1)	MIB File	New Features
V4.04.004	Update the MIBs (for DES-3200-10/10-DC/18/18-DC/26/26-DC 28/28F/28/ME/28P/52/52P C1)	Support new models-DES-3200-28/ME C1
V4.03.004	Update the MIBs (for DES-3200-10/10-DC/18/18-DC/26/26-DC 28/28F/28P/52/52P C1)	Support new models-DES-3200-18/18-DC/28F/52-DC C1
V4.02.004	Update the MIBs (for DES-3200-10/10-DC/26/26-DC/28/28P/52/52P C1)	Support new models-DES-3200-10/10-DC/26-DC C1
V4.00.024	Update the MIBs (for DES-3200-26/28/28P/52/52P C1)	Support new models-DES-3200-26/28 C1
V4.00.020	First Release (for DES-3200-28P/52/52P C1)	

Firmware Version (DES-3200 A1/B1)	MIB File	New Features
V1.28.009	NA	NA
V1.25.007	des3200ME-28-L2mgmt.mib des3200ME-28-L3mgmt.mib Equipment.mib des3200me-28-LED.mib	Those MIBs are specific for DES-3200-28/ME only
V1.21.B006	des3200-26-L2mgmt.mib des3200-26-L3mgmt.mib DV_DES-3200-26V1.21_V1.21R05-F1.21B003	Add new model DES-3200-26
	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib	<ol style="list-style-type: none"> Loopback detection: Support VLAN-based detection /shutdown 802.1ag Connectivity Fault

		Management (CFM)
	BPDUProtection.mib	BPDU Attack Protection
	nlb.mib	Network Load Balancing(NLB)
	Ie8023ah.mib	802.3ah Ethernet Link OAM
	IEEE8021-CFM-MIB.mib	Connectivity Fault Management (CFM)
	erps.mib	Ethernet Ring Protection Switching(ERPS)
	PPPoEmgmt.mib	PPPoE Circuit ID Insertion
	rfc1907.mib	Display uptime in command show_switch
	Qos.mib	Per egress queue bandwidth control
	des3200-10-L3mgmt.mib des3200-18-L3mgmt.mib des3200-28-L3mgmt.mib des3200-28f-L3mgmt.mib	DHCP option 12
	Filter.mib	DHCP Server Screening
V1.10.B015	First Release	

Changes of Command Line Interface:

The section below only shows command line changes that may bring backward compatibility issues with configuration settings for previous version of firmware. Any new feature commands that do not have backward compatibility issues are not included in the below section.

Firmware Version (DES-3200 C1)	Changes
V4.04.004	NA
V4.03.004	NA
V4.02.004	NA
V4.00.024	NA
V4.00.020	NA

Firmware Version (DES-3200 A1/B1)	Changes
V1.28.009	NA
V1.25.007	NA
V1.21.B006	<ol style="list-style-type: none">1. Change "enable authorization network" to "enable authorization attributes"2. Change "disable authorization network" to "disable authorization attributes"3. Modify the command: from save [config log all] to save {config log all}
V1.10.B015	First release

Problem Fixed:

Firmware Version (DES-3200 C1)	Problems Fixed
V4.04.004	1. When enabling OAM feature, once the connection is down, DES-3200 C1 doesn't send any SNMPtraps and write events in the log (DRU20120705000002).
V4.03.004	NA
V4.02.004	1. The FDB entry learning function can't well work in DES-3200-52 C1 with F/W 4.00.024 (DRU20120306000003)
V4.00.024	NA
V4.00.020	1. [D-View module] When user execute DES-3200 C1 D-view module via HP Open View, it will fail to close its module after turn off HP Open View program.

Firmware Version (DES-3200 A1/B1)	Problems Fixed
V1.28.009	<ol style="list-style-type: none"> The switch will enter cpu exception when the user login via SSH.(DRU20110314000001) The switch will enter cpu exception if the user deletes too many ACL rule in one time by ACL Finder page of Web UI (DRU20110322000008) When "multicast port_filtering" is configured as "filter_unregistered_groups",The PCs cannot ping each other by IPv6 address (DRU20110209000004)
V1.25.007	<ol style="list-style-type: none"> The switch cannot send AAA RADIUS request packets to RADIUS server when login via SSH (DRU20101110000001) The switch will enter EXCEPTION mode and automatically reboot if a certain "config radius" command is configured.(HQ20101206000007) When checking profile ID (show limited_multicast_addr ports) on each port via SNMP, it shows incomplete entries.(DRU20100803000003) When setting the method of lock_address_mode in Port_security module as DeleteOnTimeout, Type of FDB will show Dynamic rather than DeleteOnTimeout (DRU20100812000004) On traffic segmentation enabled ports, the packet forwarding process forwards the packet before checking if the port is in the forwarding portlist of the port's traffic segmentation portlist. (DRU20100723000004) The Port Description via web does not display correctly and does not correspond to the Port Description via CLI (DRU20100813000002) When a MAC address is already dynamically learned on the port, the permanent entry of this MAC cannot be created via SNMP operation(DRU20100827000003) SNMP group cannot be created via Web (DRU20100830000005) When MAC collision happens, the collided client that is not in the switch's FDB table can not get IP configuration via DHCP (DRU20100630000008) In MSTP setting, ping traffic in a VLAN with a non-CIST MSTP instance will fail (DRU20100708000004)

	<ol style="list-style-type: none"> 11. The traffic segmentation does not take effect in DES-3200-18 and DES-3200-10 GE ports (ie, 17-18, and 9-10, respectively) (DRU20100723000004) 12. The switch is not able to return value correctly in certain SNMPwalk operations (DRU20100520000003) 13. The switch cannot successfully save configuration via WebUI in Linux platform (DRU20100531000002) 14. The Clients can not get IP from the DHCP server sometimes when connecting to the switch. (DRU20100429000003) 15. ERPS/STP/802.1x discarding ports are not masked out from the forwarding ports and those ports do not drop ARP/IP packets received in discarding ports so that the switch show incorrect FDB entry (DRU20100514000005) 16. Inappropriate memory management causes that the switch enters exception mode when executing some snmpwalk commands (DRU20100518000003) 17. Inappropriate memory management causes that the switch enters exception mode when trying to get LLDP data via snmp (HQ20100412000012) 18. Loop back detection(LBD) packets are treated as unauthorized packets by MAC Access Control/802.1X, which causes LBD not to work (HQ20100420000005) 19. The switch can not upload/download configuration or logs via WebUI when using Firefox 3.62 (HQ20100331000002)
<p>V1.21.B006</p>	<ol style="list-style-type: none"> 1. The ACL counter function does not work properly when creating an ACL counter with c_tag (DI20100120000014) 2. If adding ACL rules with the same examination part such as ethernet type to 2 profiles respectively, the switch pops up the warning message "A similar profile already exists with profile_id 1!". The ACL configuration will fail. (DI20100122000012) 3. A legal ping packet destined to x.x.254.255/16 is treated as smurf attack and is dropped by the switch (DI20091023000003) 4. When creating an ACL profile by two different command orders via SNMP, the ACL profile works only can work one SNMP command order (DI20091028000022) 5. While creating packet content filtering ACL rule via WebUI, the Profile can be created but the access_id can not be created (DI20091102000023) 6. When ISM VLAN, 802.1X, and Guest VLAN are enabled on a port, the port can't follow to pass multicast if the port is authenticated by 802.1X. (DI20091110000021) 7. The switch will lose the access_id setting in ACL after saving configuration and rebooting the switch (DI20091123000011) 8. The switch does not drop invalid IGMP join packet when the destination MAC address of IGMP join packet is not the same as joined multicast group (DI20091208000017) 9. Jumbo frame status is not synchronized between CLI and WEB. When jumbo_frame is enabled via CLI, the WEB still displays "jumbo_frame disable" (DI20091215000020) 10. When creating an ACL profile with L2 and L3 parts, the switch will display L3 and L4 part in the created profile (DI20091215000023) 11. When setting the flow_meter, traffic rate's flapping range is not precise. For example, setting 1000kbps, but the flap ranges between (494kb to 1311 kb) (DI20090828000018). Please refer to the known issue in firmware version V1.10.B015.
<p>V1.10.B015</p>	<p>First Release</p>

Known Issues:

Firmware Version (DES-3200 C1)	Issues	Workaround
V4.04.004	<ol style="list-style-type: none"> 1. [SSH]When using "Config ssh server rekey()" to specify time to regenerate session key, the behavior of time setting will be "always". 2. [OAM]When the link of physical port is link down, "Ethernet oam port x event log ()" will not display event log in Critical Event Local. Also, the device will not encounter an OAM critical event. 3. [FFS] The "rd" command is used to delete a directory in the file system. If there are files existing in the directory, this command will fail to execute and return an error message. In FW v4.04.004, the file attribute will be changed* once using "rd" command to delete this directory (*: The file backup attribute will be removed). 4. [MLD snooping]When the device is configured to MLDv1 version and gets the MLDv2 version query packet with the lower IP address, the system will show error. 5. [DHCP Relay] When client releases a DHCP IP address and configures a static IP, the DHCP release packet will not be relayed 6. [802.1X] Accounting will not work for each host when 802.1X mac_based mode is enabled. (* : Once 802.1X mac_based mode is enabled, it will present the same behavior as user enabling 802.1X port_based mode) 7. [SNMP]In IWL testing, when the mib node "smtpTestMsgContent" (Size list: 1: 0..512) set the input string length as "512", string length still can't be longer than 256 characters. 8. [802.1X]When using PEAP authentication, the field of accounting user name is wrong. (Now the user name field is "outer name" (incorrect), not "inner name"(correct). 9. [Filed case-TFTP] Switch can't upload the configuration file to specific TFTP server (pumpkin v2.7.2). 10. [MBA]When the client moves from MBA(MAC-Base Authentication) enabled port to the other non-MBA(Mac-Base Authentication) port, FDB entry will not be cleared 11. [IGMP_snooping] The behavior of IGMP_snooping data_driven_group learning was incorrect. 	

	<ol style="list-style-type: none"> 12. [QinQ] When user uses "config qinq ports x-x role uni outer_tpid 0x8100", the switch will recognize the incoming packets(inner tpid usually is 0x8100) as outer tagged and we will drop the packet. 13. When user uses Telnet or SSH connection: once IP address is changed, switch doesn't send "termination" packet to inform user even Telnet or SSH connection is closed. 14. [SSH]If there are more than 1 SSH connection established, some connection sessions' level will be changed. 15. [IPv6]When "IPv6" is disabled (default) or "config multicast vlan_filtering" mode is set as "filter_unregistered_groups", it will fail to forward ICMPv6 with DA=33-33-XX-XX-XX-XX packet 	
<p>V4.03.004</p>	<ol style="list-style-type: none"> 1. [SSH]When using "Config ssh server rekey()" to specify time to regenerate session key, the behavior of time setting will be "always". 2. [OAM]When the link of physical port is link down, "Ethernet oam port x event log ()" will not display event log in Critical Event Local. Also, the device will not encounter an OAM critical event. 3. [FFS] The "rd" command is used to delete a directory in the file system. If there are files existing in the directory, this command will fail to execute and return an error message. In FW v4.04.004, the file attribute will be changed* once using "rd" command to delete this directory (*: The file backup attribute will be removed). 4. [MLD snooping]When the device is configured to MLDv1 version and gets the MLDv2 version query packet with the lower IP address, the system will show error. 5. [DHCP Relay] When client releases a DHCP IP address and configures a static IP, the DHCP release packet will not be relayed 6. [802.1X] Accounting will not work for each host when 802.1X mac_based mode is enabled. (* : Once 802.1X mac_based mode is enabled, it will present the same behavior as user enabling 802.1X port_based mode) 7. [SNMP]In IWL testing, when the mib node "smtpTestMsgContent" (Size list: 1: 0..512) set the input string length as "512", string length still can't be longer than 256 characters. 8. [802.1X]When using PEAP authentication, the field of accounting user name is wrong. (Now the user name field is "outer name" (incorrect), not "inner name"(correct). 9. [Filed case-TFTP] Switch can't upload the 	<p>NA</p>

	<p>configuration file to specific TFTP server (pumpkin v2.7.2).</p> <ol style="list-style-type: none"> 10. [MBA]When the client moves from MBA(MAC-Base Authentication) enabled port to the other non-MBA(Mac-Base Authentication) port, FDB entry will not be cleared 11. [IGMP_snooping] The behavior of IGMP_snooping data_driven_group learning was incorrect. 12. [QinQ] When user uses "config qinq ports x-x role uni outer_tpid 0x8100", the switch will recognize the incoming packets(inner tpid usually is 0x8100) as outer tagged and we will drop the packet. 13. When user uses Telnet or SSH connection: once IP address is changed, switch doesn't send "termination" packet to inform user even Telnet or SSH connection is closed. 14. [SSH]If there are more than 1 SSH connection established, some connection sessions' level will be changed. 15. [IPv6]When "IPv6" is disabled (default) or "config multicast vlan_filtering" mode is set as "filter_unregistered_groups", it will fail to forward ICMPv6 with DA=33-33-XX-XX-XX-XX packet 	
<p>V4.02.004</p>	<ol style="list-style-type: none"> 1. [SSH]When using "Config ssh server rekey()" to specify time to regenerate session key, the behavior of time setting will be "always". 2. [OAM]When the link of physical port is link down, "Ethernet oam port x event log ()" will not display event log in Critical Event Local. Also, the device will not encounter an OAM critical event. 3. [FFS] The "rd" command is used to delete a directory in the file system. If there are files existing in the directory, this command will fail to execute and return an error message. In FW v4.04.004, the file attribute will be changed* once using "rd" command to delete this directory (*: The file backup attribute will be removed). 4. [MLD snooping]When the device is configured to MLDv1 version and gets the MLDv2 version query packet with the lower IP address, the system will show error. 5. [DHCP Relay] When client releases a DHCP IP address and configures a static IP, the DHCP release packet will not be relayed 6. [802.1X] Accounting will not work for each host when 802.1X mac_based mode is enabled. (* : Once 802.1X mac_based mode is enabled, it will present the same behavior 	<p>NA</p>

	<p>as user enabling 802.1X port_based mode)</p> <ol style="list-style-type: none"> 7. [SNMP]In IWL testing, when the mib node "smtpTestMsgContent" (Size list: 1: 0..512) set the input string length as "512", string length still can't be longer than 256 characters. 8. [802.1X]When using PEAP authentication, the field of accounting user name is wrong. (Now the user name field is "outer name" (incorrect), not "inner name"(correct). 9. [Filed case-TFTP] Switch can't upload the configuration file to specific TFTP server (pumpkin v2.7.2). 10. [MBA]When the client moves from MBA(MAC-Base Authentication) enabled port to the other non-MBA(Mac-Base Authentication) port, FDB entry will not be cleared 11. [IGMP_snooping] The behavior of IGMP_snooping data_driven_group learning was incorrect. 12. [QinQ] When user uses "config qinq ports x-x role uni outer_tpid 0x8100", the switch will recognize the incoming packets(inner tpid usually is 0x8100) as outer tagged and we will drop the packet. 13. When user uses Telnet or SSH connection: once IP address is changed, switch doesn't send "termination" packet to inform user even Telnet or SSH connection is closed. 14. [SSH]If there are more than 1 SSH connection established, some connection sessions' level will be changed. 15. [IPv6]When "IPv6" is disabled (default) or "config multicast vlan_filtering" mode is set as "filter_unregistered_groups", it will fail to forward ICMPv6 with DA=33-33-XX-XX-XX-XX packet 	
<p>V4.00.024</p>	<ol style="list-style-type: none"> 1. [SSH]When using "Config ssh server rekey()" to specify time to regenerate session key, the behavior of time setting will be "always". 2. [OAM]When the link of physical port is link down, "Ethernet oam port x event log ()" will not display event log in Critical Event Local. Also, the device will not encounter an OAM critical event. 3. [FFS] The "rd" command is used to delete a directory in the file system. If there are files existing in the directory, this command will fail to execute and return an error message. In FW v4.04.004, the file attribute will be changed* once using "rd" command to delete this directory (*: The file backup attribute will be removed). 4. [MLD snooping]When the device is 	<p>NA</p>

	<p>configured to MLDv1 version and gets the MLDv2 version query packet with the lower IP address, the system will show error.</p> <ol style="list-style-type: none"> 5. [DHCP Relay] When client releases a DHCP IP address and configures a static IP, the DHCP release packet will not be relayed 6. [802.1X] Accounting will not work for each host when 802.1X mac_based mode is enabled. (* : Once 802.1X mac_based mode is enabled, it will present the same behavior as user enabling 802.1X port_based mode) 7. [SNMP]In IWL testing, when the mib node "smtpTestMsgContent" (Size list: 1: 0..512) set the input string length as "512", string length still can't be longer than 256 characters. 8. [802.1X]When using PEAP authentication, the field of accounting user name is wrong. (Now the user name field is "outer name" (incorrect), not "inner name"(correct). 9. [Filed case-TFTP] Switch can't upload the configuration file to specific TFTP server (pumpkin v2.7.2). 10. [MBA]When the client moves from MBA(MAC-Base Authentication) enabled port to the other non-MBA(Mac-Base Authentication) port, FDB entry will not be cleared 11. [IGMP_snooping] The behavior of IGMP_snooping data_driven_group learning was incorrect. 12. [QinQ] When user uses "config qinq ports x-x role uni outer_tpid 0x8100", the switch will recognize the incoming packets(inner tpid usually is 0x8100) as outer tagged and we will drop the packet. 13. When user uses Telnet or SSH connection: once IP address is changed, switch doesn't send "termination" packet to inform user even Telnet or SSH connection is closed. 14. [SSH]If there are more than 1 SSH connection established, some connection sessions' level will be changed. 15. [IPv6]When "IPv6" is disabled (default) or "config multicast vlan_filtering" mode is set as "filter_unregistered_groups", it will fail to forward ICMPv6 with DA=33-33-XX-XX-XX-XX packet 	
V4.00.020	<ol style="list-style-type: none"> 1. [SSH]When using "Config ssh server rekey() to specify time to regenerate session key, the behavior of time setting will be "always". 2. [OAM]When the link of physical port is link down, "Ethernet oam port x event log ()" will not display event log in Critical Event Local. Also, the device will not encounter an 	NA

- OAM critical event.
3. [FFS] The "rd" command is used to delete a directory in the file system. If there are files existing in the directory, this command will fail to execute and return an error message. In FW v4.04.004, the file attribute will be changed* once using "rd" command to delete this directory (*: The file backup attribute will be removed).
 4. [MLD snooping]When the device is configured to MLDv1 version and gets the MLDv2 version query packet with the lower IP address, the system will show error.
 5. [DHCP Relay] When client releases a DHCP IP address and configures a static IP, the DHCP release packet will not be relayed
 6. [802.1X] Accounting will not work for each host when 802.1X mac_based mode is enabled. (* : Once 802.1X mac_based mode is enabled, it will present the same behavior as user enabling 802.1X port_based mode)
 7. [SNMP]In IWL testing, when the mib node "smtpTestMsgContent" (Size list: 1: 0..512) set the input string length as "512", string length still can't be longer than 256 characters.
 8. [802.1X]When using PEAP authentication, the field of accounting user name is wrong. (Now the user name field is "outer name" (incorrect), not "inner name"(correct).
 9. [Filed case-TFTP] Switch can't upload the configuration file to specific TFTP server (pumpkin v2.7.2).
 10. [MBA]When the client moves from MBA(MAC-Base Authentication) enabled port to the other non-MBA(Mac-Base Authentication) port, FDB entry will not be cleared
 11. [IGMP_snooping] The behavior of IGMP_snooping data_driven_group learning was incorrect.
 12. [QinQ] When user uses "config qinq ports x-x role uni outer_tpid 0x8100", the switch will recognize the incoming packets(inner tpid usually is 0x8100) as outer tagged and we will drop the packet.
 13. When user uses Telnet or SSH connection: once IP address is changed, switch doesn't send "termination" packet to inform user even Telnet or SSH connection is closed.
 14. [SSH]If there are more than 1 SSH connection established, some connection sessions' level will be changed.
 15. [IPv6]When "IPv6" is disabled (default) or "config multicast vlan_filtering" mode is set as "filter_unregistered_groups", it will fail to

forward ICMPv6 with
DA=33-33-XX-XX-XX-XX packet

Firmware Version (DES-3200 A1/B1)	Issues	Workaround
V1.28.009	NA	NA
V1.25.007	NA	NA
V1.10.B015	TCP traffic on per-flow bandwidth control is inaccurate	Upgrade to V1.10.B016 or above, but only in the situation that the bandwidth is less than 10M.

Related Documentation:

- DES-3200 Series R4.04 H/W Installation Guide
- DES-3200 Series R4.04 CLI Reference Guide
- DES-3200 Series R4.04 Web UI Reference Guide

- DES-3200 Series R1.28 H/W Installation Guide
- DES-3200 Series R1.28 CLI Manual
- DES-3200 Series R1.28 User Manual