Firmware Version: v10.4(3)
Published: July 8, 2011

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	Chassis Model	Control Model	Hardware Version
v10.4(3)	8-July-2011	DES-7206 DES-7210	7200-CM1	A1, A2, A3
			7200-CM2	A1, A2, A3
			7200-CM3	A1, A2, A3
			7200-CM4	A1, A2, A3
v10.3(5)	31-Dec.-2009	DES-7206	7200-CM1	A1, A2, A3
			7200-CM3	A1, A2, A3
		DES-7210	7200-CM2	A1, A2, A3
			7200-CM4	A1, A2, A3
v10.3(3b19)	10-Apr.-2009	DES-7206	7200-CM1	A1
			7200-CM3	A1
		DES-7210	7200-CM2	A1
			7200-CM4	A1
v10.2(2)	10-May-2008	DES-7206	7200-CM1	A1
			7200-CM3	A1
		DES-7210	7200-CM2	A1
			7200-CM4	A1
v10.1(4)	7-Aug.-2007	DES-7206	7200-CM1	A1
		DES-7210	7200-CM2	A1
v10.0	22-Apr.-2007	DES-7206	7200-CM1	A1
		DES-7210	7200-CM2	A1

Firmware Version	Supported Line Cards				
v10.4(3)	7200-24G	7200-24	7200-2XG	7200-24P	7200-48
	7200-4XG	7200-48P	7200-ASE3	7200-24GE	7200-24G2XG
v10.3(5)	7200-24G	7200-24	7200-2XG	7200-24P	7200-48
	7200-4XG	7200-48P	7200-ASE3	7200-24GE	7200-24G2XG
v10.3(3b19)	7200-24G	7200-24	7200-2XG	7200-24P	7200-48
	7200-4XG	7200-48P	7200-ASE3	7200-24GE	
v10.2(2)	7200-24G	7200-24	7200-2XG	7200-24P	7200-48
	7200-4XG	7200-48P			
v10.1(4)	7200-24G	7200-24	7200-2XG	7200-24P	7200-48

	7200-4XG				
v10.0	7200-24G	7200-24	7200-2XG		

Upgrade Instructions:

DES-7200 supports 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.

Operating Principle

The firmware image release for DES-7200 devices is a self-extracting executable program. It carries main program and boot program for both chassis devices and modules.

During the upgrade process, the user will first need to operate in the file system to copy the new-version firmware image to the device. During the installation process, the system will automatically search for image to be upgraded and upgrade them one by one. The system will automatically guarantee the compatibility of respective images after the upgrade. No further identification by the user is needed.

In case a line card is plugged when the device is still running, the service of this line card will be started if the system detects that this line card is compatible with the program image of current device, or use the line card program image contained in the firmware image stored in the master control module (CM) to upgrade this line card or download the image if incompatible. The line card will be reset after the upgrade (no need to reset during image download) and will then enter into ready state. For such devices, the image used by line card or slave board always needs to maintain compatible with the program run on the master CM.

The user may choose two ways for system upgrading. The corresponding processes are shown below:

Manual upgrade (Recommended): Copy new firmware to the device -> input install command -> reset device
Automatic upgrade: Copy new firmware to the device -> reset device -> wait until device installation is completed

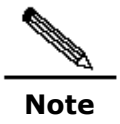
The advantage of manual upgrade is to shorten the service down time and provide higher reliability. It allows users pre-install the firmware to all the modules without impact the operation of the system. If any accident incurs during the pre-installation, as long as the device is still powered on, the installation operation can be repeated without leading to any risk. Once the installation is completed successfully, the device can function immediately after reboot.

The automatic upgrade is easy to operate, and no intervention by user is needed once the upgrade process commences. However it takes longer time for first restart of system upgrade.

Note

If the current boot/main program of master CM is upgraded, this upgrade file will also upgrade and replace the boot/main program of slave CM. However, if ISSU function is enabled, the system will no longer automatically upgrade the boot program of slave CM, and manual upgrade by the user will be needed.

Preparation before upgrade



Note

The switch serial port default settings are as follows:

- Baud rate: **9600**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**

Make the following preparations before implementing device upgrade:

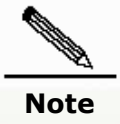
1. Confirm the file system has enough space for firmware files.
2. Make sure the CPU utilization is lower than 20%, or the upgrade process may get failed.
3. Backup the configuration files.

The user may use following commands to learn the space and its usage of the existing file system.

Command	Function
`show file systems`	Display the file systems supported in the present devices and the available space condition in the file system.
`dir [`*`filesystem:`*`][`*`directory`*`]`	Enter the specified directory to show the information of all the files in that directory. If no parameter is specified, the information of the files in the present directory is shown by default. The possible filesystems are: **flash:** Flash of master CM **slave:** Flash on the slave CM **usb0:** USB driver plugged on master CM **sd0:** SD card plugged on master CM

If the target file system has sufficient space to store both new and old program images, then during the upgrade process, the original boot/main program will be renamed as "*original filename*.bak". When the new program image fails, the system will boot with this backup image. This can save the rollback operation required in the case of upgrade failure.

When the system has hardly any residual space, the user will need to clean up the file system in order to make sure the upgrade is successful. Unnecessary files can be deleted using "del" command. While upgrading cabinet device with dual management boards, the file system space of the slave board shall also be verified. The URL prefix of file system space of the slave board is "slave:".



Note

Caution When file system space is insufficient to store two program images, the backup file of original program image will not be generated.

After checking the file system space. The user may use following commands to check CPU utilization of the existing file system.

Command	Function
`show CPU`	Display the system CPU utilization information in 5sec, 1 min and 5 min,

Caution

Do not upgrade the line card or plug/reset the line card when the device is extremely busy (with CPU utilization rate > 70%). This may lead to unsuccessful upgrade or boot failure of line card.
If automatic upgrade of line card or image distribution is failed. Please try to reset the line card again after the CPU utilization goes down, until the line card is successfully upgraded or booted.
If the upgrade is failed due to high CPU utilization, the user will need to retry manual upgrade after the CPU utilization goes down.

Backup of configuration files is needed before the upgrade. Since different versions of software may contain different default configurations, the newly added default configurations may conflict with the current configurations. In order to ensure successful upgrade, please backup the original configuration file before the upgrade. After successful upgrade, verify whether there is any conflict in configurations.

The user may use following commands to backup the configuration files for firmware images.

Command	Function
`copy <source-url> <destination-url>`	Copy a file from the specified source directory to the specified destination directory. The possible url are: **flash:** Flash of master CM **tftp:** TFTP network server **xmodem:** Device connected through console **slave:** Flash on the slave CM **usb0:** USB driver plugged on master CM **sd0:** SD card plugged on master CM

Download Firmware

By default, DES-7200 uses flash:/firmware.bin as the boot image. The user may use "copy" command to replace the original boot image.

DES-7200 supports 4 ways for firmware download. See below for the detailed instructions:

Download Firmware via TFTP server (Recommended)

When user uses TFTP to download firmware from tftp server to the device (master CM) and at the same time overwrites the boot/main program, the system will check the validity of the upgrade file downloaded (i.e., whether inappropriate upgrade file is downloaded, or whether the upgrade file is corrupted). Upgrading of boot/main program via other means (such as ftp, Xmodem and other file system commands) will not result in validity check. Therefore, for safety reason, it is recommended using TFTP to overwrite the boot image (master CM) of the device.

When the device is plugged with two CM, use "copy tftp" command will synchronize this upgrade file to the slave CM automatically. If the user doesn't want to use this download method, for device like DES-7200, it is recommend using manual installation ("upgrade system" installation command) after copying the upgrade file to the device. Manual installation is safer, and allows the user to quickly discover image problems and timely correct such problems.

Note

Using TFTP overwrite the boot image of slave board won't lead to the corresponding check as well.

Note

Some TFTP servers only support the transfer of files with size below 32M. If the file size is larger than 32M, the file might have to be downloaded via FTP or flash disk.

Download Firmware via Xmodem

Xmodem download is applicable to some exceptional cases, such as the failure in network connection. Before using xmodem download, make sure the device is linked to console with serial line. In order to obtain faster download speed, the baud rate of connection can be increased. At the same time, make sure the terminal software supports xmodem transmission.

Note

The user will need to manually copy the upgrade file to the slave CM to overwrite the boot image when using Xmodem.

Download Firmware via FTP

Set the device as FTP server, and use FTP client to download upgrade file.

Note

The user will need to manually copy the upgrade file to the slave CM to overwrite the boot image when using FTP.

Copy via flash disk

Plug the flash disk stored with firmware image to the USB port. Make sure the device has found this USB apparatus.

Note

The user will need to manually copy the upgrade file to the slave CM to overwrite the boot image when copying upgrade file from flash disk.

Upgrade Process

Manual Upgrade (Recommended)

To ensure reliable upgrade, it is recommended upgrading the system by manual upgrade process. Following commands are required for the manual upgrade.

Command	Function
`copy <source-url> <destination-url>`	Copy a file from the specified source directory to the specified destination directory. The possible url are: **flash:** Flash of master CM **tftp:** TFTP network server **xmodem:** Device connected through console **slave:** Flash on the slave CM **usb0:** USB driver plugged on master CM **sd0:** SD card plugged on master CM
`upgrade system <filename>`	Manual upgrade the system by using specific firmware file.

The following is the example (TFTP) of manual upgrade:

```
DES-7200#copy tftp://192.168.201.98/DES7200-V10.4(3)-R118875.bin flash:firmware.bin
Accessing tftp://192.168.201.98/firmware.bin...
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
Verify the system boot image .....[ok]
Upgrading system boot image on slave:/
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 21,525,888 bytes]
Waiting for image installed........Complete

CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20060062
  PRODUCT DESCRIPTION: DES-7200 High-density IPv6 10G Core Routing Switch

SUCCESS: UPGRADING OK.
DES-7200#
```

After the new-version software is successfully downloaded to the device, use "upgrade" command to upgrade the system:

```
DES-7200#upgrade system firmware.bin
These images in linecard will be updated:
    Slot    image    linecard
    ----    -----    ----------------
       1    MAIN    7200-24
       6    MAIN    7200-24G
-------------------------------------
(Slot 1): Installing MAIN
(Slot 1): Download image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!![OK - 8,003,872 bytes]
Waiting for image installed....Complete
(Slot 1): MAIN installed.
(Slot 1): All images have been installed.
(Slot 6): Installing MAIN
(Slot 6): Download image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![
OK - 8,003,872 bytes]
Waiting for image installed....Complete
(Slot 6): MAIN installed.
(Slot 6): All images have been installed.
DES-7200# reload
Proceed with reload? [no] Yes
```

After the device is reload, the device will be running the new-version software.

Automatic Upgrade
The automatic upgrade is easy to operate, but with longer time system restart period. See below for the example (TFTP) of automatic upgrade:

```
DES-7200#copy tftp://192.168.201.97/firmware.bin flash:firmware.bin
Accessing tftp://192.168.201.97/firmware.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Checking file, please wait for a few
minutes ....
Check file success.

Transmission finished, file length 22655264

THE PROGRAM VERSION: firmware 10.4.*, Release(64046)

Upgrade file to Module(s) in slot: [M2]
Please wait......
Upgrade file to Module in slot [M2] OK!
Upgrade Master CM main program OK.

CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20060062
  PRODUCT DESCRIPTION: DES-7200 High-density IPv6 10G Core Routing Switch

SUCCESS: UPGRADING OK.
DES-7200#reload
Proceed with reload? [no] Yes
```

After the device is reload, the device process the system upgrade automatically.

Dynamic Linecard Plug-in

When line card is dynamically inserted to DES-7200, the system will automatically check the software version of this line card. If its software version is incompatible with that of the system, this card will be automatically upgraded by the system before operation.

The following is the example of dynamically inserting a line card:

```
*Apr  2 07:39:06: %UPGRADE-5-DISPATCH_BEGIN: Dispatch image to slot 3.
Download image to slot 3: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!![OK - 8,007,680 bytes]
Waiting for image installed....Complete
```

However, if the line card is not supported by the existing firmware, the system will prompt:

```
UPGRADE-4-CARDNOTSUPPORT: The linecard in slot 1/4 is not supportted by current version.
```

Verify Device Installation

After the system installation, the user may use the show version command to verify the conditions of device upgrade, and make sure the version of main program is same as the anticipated version. It is normal that the versions of BOOT, CTRL and Bootloader programs and the image of line card may be different from the version of the main program package.
The displayed main program version indicates the version number of main program being run in the system. Therefore, in the case of manual installation, the displayed version number of main program is not the version number of software newly installed, but the version number of software run currently.

For chassis device, if the line card automatic upgrade process begins, the line card will be reset and execute the new program. The user needs to wait until the line card enters into UP state and then uses show version command to verify its version number.

Common Upgrade Problems

Loss of Main Program of Master Management Board

The user may accidentally delete the boot/main program of the file system, and the system will give the following warning information:

```
Warning: System boot file firmware.bin is missing.
```

If the user doesn't notice such loss of main program and dynamically inserts a new line card during the subsequent use, the system will prompt:

```
*Aug 25 13:21:50: %UPGRADE-3-DISPATCH_FAIL: Dispatch program to slot 3 failed.
```

Unsupported Line cards

If the line card detected be device is not supported by the current firmware version, the system will prompt:

```
*Jan 2 00:00:39: %UPGRADE-4-CARDNOTSUPPORT: The linecard in slot [dec/dec/...] is not
supportted by current version.
```

In such a case, support to such type of line card as specified in the release of current software version shall be verified. If this line card needs to be supported, then the current software shall be upgraded.

Insufficient File System Space

Insufficient file system space may take place during download or file copying. The system will prompt:

```
Insufficient file system space。
```

By this time, useless files on the file system shall be cleaned up. For device with smaller file system space, the current boot/main program can be deleted as long as the device is powered on, and then use "copy tftp" command to copy the new upgrade file to the device as the new boot/main program.

Boot/main Program not Overwritten during Upgrade

If the boot/main program is not upgraded during the upgrade, the new program will not run after system reboot.
As for the slave board, please verify the name of boot/main program before upgrade. If the boot/main program is not upgraded, the software versions of master and slave boards may be inconsistent after system reboot.

Timeout Failure Displayed during Upgrade

The timeout failure may be displayed during the upgrade.

```
*Feb 10 15:47:12: %UPGRADE-4-PROTO_TIMEOUT: Server is busy and ack timeout.
```

By this time, the following solutions can be used:
1. Ensure whether the modules to be upgraded are plugged or reset.
2. Ensure whether the modules to be upgraded are busy (with high CPU utilization rate)
3. Ensure whether the modules to be upgraded are using large file system space, if so, remove some useless files, and retry the upgrade after freeing the file system space.

New Features:

Firmware Version	New Features
v10.4(3)	1. BGP AS 32 2. Support user-defined NFPP 3. VRRP V3 4. Web GUI 5. GVRP
v10.3(5)	1. Support the dynamic LACP function. 2. Configurable VLAN ID changes from 1-4093 to 1-4094 3. Selective Q in Q 4. Root Guard 5. Loop Guard 6. Supports the MSTP interconnection with Cisco Catalyst 3550 12.2(25)SEC or later). Flow-based and one-to-many port mirroring. 7. Dynamic VLAN assignment for 802.1X after successful authentication. 8. Identity Driven ACL for 802.1X 9. TACACS+ for Management Access
v10.3(3b19)	1. VLAN-based ACL for Enhanced I/O Module 2. IP Source Guard 3. Support the MPLS(L3 VPN), which requires 7200-ASE3 4. VRF: 5. VRF-aware DHCP 6. VRF-aware SNMP 7. VRF-aware Syslog 8. VRF-aware AAA 9. VRF-aware TACACS+ 10. VRF-aware tftp
v10.2(2)	1. Alias option for command line. 2. Include/exclude option for show commands. 3. Support show command in all modes of CLI. 4. Cable Diagnostics 5. Support link state check for LACP member ports. 6. Auto Edge Port function for MSTP. 7. PIM Snooping 8. IGMP Proxy
v10.1(4)	1. PIM-SM 2. Bgp4 3. RLDP
v10.0	First release, please refer to datasheet and manual for detailed information of supported functions.

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
v10.4(3)	No changes	
v10.3(5)	No changes	
v10.3(3b19)	rfc2737.mib	Add Entity MIB

	MY-PIM-MIB.mib	Add PIM MIB
v10.2(2)	rfc2906.mib	Add IP FDB MIB
	MY-BGP4-MIB.mib zebos_BGP4_MIB	Add BGP4 MIB
	rfc1643.mib	Add Ether-like MIB
	ospf_1850.mib ospf_1850_trap.mib MY-OSPF-MIB.mib	Add OSPFv2 MIB
	rfc2021.mib	Add RMON2 MIB
	p-bridge.mib q-bridge.mib	Add Q-Bridge, P-Bridge MIB
v10.1(4)	No changes	
v10.0	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
v10.4(3)	No changes
v10.3(5)	No changes
v10.3(3b19)	No changes
v10.2(2)	No changes
v10.1(4)	No changes
v10.0	First release

Problem Fixed:

Fixed Revision	Problems Fixed
v10.4(3)	1. The L2 multicast address resolution will be incorrect when both L2 multicast and L3 multicast are enabled concurrently
v10.3(5)	1. The PC is out of network due to the default route failure if you do all the following configurations: ◆ Set policy-map QoS which associates 3 extended ACL (11 ACEs) with 1 standard ACL including 1 ACE on 2 Trunk ports and 1 physical port. ◆ Set the same extended ACL including 16 ACEs and default deny any on 27 SVIs. ◆ Learn a default route through OSPF. 2. Enabling Super VLAN and PBR at the same time leads to PBR failure. 3. The user with legal IP address cannot telnet the switch under all the following conditions: ◆ A standard or extended ACL that only permits some source IP addresses has been configured in the global configuration mode. ◆ The access-class <acl-num> in command has been executed to associate that ACL in line vty mode to allow the specified user to telnet the switch,

	but to prevent other users from telneting.
	◆ A numbers of illegal users in the network are trying to telnet the switch.
	4. IGMP SNOOPING and PIM cannot be enabled at the same time.
	5. The switch will auto-reload when route entries exceed switch route-table capacity.
	6. The blocked LACP port is in the Forwarding state with LACP enabled but STP disabled which will result in the loop and broadcast storm on the interface.
	7. When the following configurations have been executed, it will cause that the memory is reduced bit by bit. Finally, the available memory of the switch will be insufficient and the authentication will fail. The user is unable to obtain the IP address and access the network.
	◆ Enable the dhcp function:
	`DES-7200(config)#service dhcp`
	◆ Enable the option dot1x function:
	`DES-7200(config)#ip dhcp relay information option dot1x`
	◆ Enable the dot1x authentication function on the switch port:
	`DES-7200 (config)#interface gigabitEthernet 0/1`
	`DES-7200 (config-if-GigabitEthernet 0/1)#dot1x port-control auto`
	◆ The user connecting to the dot1x authentication port applies for or releases the IP address dynamically.
	8. The ACL is invalid for the routing packets under the following conditions:
	◆ The egress ACL on the SVI (suppose it is SVI2) has been configured.
	◆ The routing packets are sent into a trunk port and forwarded through another SVI2 port

v10.3(3b19)	1. The switch might experience a failure when dpackage with the name firmware (for CMII).bin using command copy tftp. 2. With active/standby switchover, IP scanning and ARP attack, if PIM-SM is enabled, the console is out of running for 30 minutes when you execute command clear ip igmp group or related show command after clear ip igmp group. If rp-address is set as the one not for the switch itself and there are 600 multicast core entries, including the directly-connected source and indirectly-connected source and 1000 ipmp groups, the console is out of running for 5 minutes. (DI20081013000009) 3. If the number of standard ACE in ACL exceeds 1535 or the standard ACL is used with Extended/Expert ACL together, the traffic can not be forwarded according to the hit default routing. 4. If the chassis is inserted with greater than or equal to 2 linecards, one of which resets in CLI or by first pulling out then plugging in or resets abnormally, the traffic can not be forwarded according to the default routing of the linecard. 5. When the length of remote vlan list on the trunk port is 256 characters, the switch crashes if you execute command show running-config or write. 6. The switch crashes if you execute command show logging when the system exports logs. 7. If the chassis is inserted with greater than or equal to 2 linecards, one of which resets in CLI or by first pulling out then plugging in or resets abnormally, the traffic can not be forwarded according to the default routing of the linecard. 8. When the length of remote vlan list on the trunk port is 256 characters, the switch crashes if you execute command show running-config or write. 9. The switch crashes if you execute command show logging when the system exports logs. 10. Set the ACL to line vty. You experience a login failure if you key in valid username but incorrect password. When you telnet using illegal IP address, the login log displays the Telnet Login failure information.

	(DI20081030000008)
v10.2(2)	1. Fix the wrong company OID. 2. Fix the MIB "Get Next" function for not work properly. 3. Fix the wrong returned value while users try to get the information from "my-powerstate" object in "MYSYSTEM" MIB. 4. Fix the Ping abnormal issue. If the ping issuer or target has been shifted to another switch port, ping will fail even they are still in same IP interface.
v10.1(4)	None

* D-Link tracking number is enclosed in ()

Known Issues:

Firmware Version	Issues	Workaround
v10.4(3)	None	None
v10.3(5)	When setting up EBGP neighbor between DES-7200 and the neighboring device, supposing 180k BGP route, 100 OSPF routes have been configured on DES-7200 and a static route has been set from DES-7200 to the neighboring device, DES-7200 will switch to MPLS mode and cancel the 180k BGP route, leading to dead forwarding for 100 OSPF routes and the static route and inconsistency between high and low layers.	1. OSPF routes could be forwarded using command: `clear ip ospf pro` 2. Layers could be consistent using command: `ip ref synchronize all`
	Only the ports on 7200-24GE could be used as the intermediate switch port to apply RSPAN feature.	None
	One RSPAN destination port can only belong to one session.	None
	When enabling PIM and IGMP SNOOPING at the same time, 2 problems occur: ◆ PIM and IGMP SNOOPING SVGL mode cannot coexist. ◆ PIM and IGMP SNOOPING Source IP check cannot coexist.	None
	System allows N routed ports and 4094-N VLANs. System will create an idle VLAN automatically when a routed port is created. If the VID of new created VLAN is occupied by idle VLANs, the system will return error message. See below for the rule of idle VLAN: ◆ Each Layer-3 AP requires 1 idle VLAN ◆ Executing label-switching command once or for multiple times consumes 1 idle VLAN	None
	The igmp report packets cannot be forwarded in the VLAN which connects to the upstream multicast router with IGMP SNOOPING disabled when L2 and L3 multicast coexist in the switch.	Fixed in v10.4(3)

Related Documentation:

- DES-7200 User Manual v10.4(3)
- DES-7200 CLI Manual v10.4(3)
- DES-7200 Hardware Installation Guide V1.4