Firmware Version: v10.3(5)
Published: 2009/12/31

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 Upgrading 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
v10.3(5)	2009/12/31	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)	2009/4/10	DES-7206	7200-CM1	A1
			7200-CM3	A1
		DES-7210	7200-CM2	A1
			7200-CM4	A1
v10.2(2)	2008/5/10	DES-7206	7200-CM1	A1
			7200-CM3	A1
		DES-7210	7200-CM2	A1
			7200-CM4	A1
v10.1(4)	2007/8/7	DES-7206	7200-CM1	A1
		DES-7210	7200-CM2	A1
v10.0	2007/4/22	DES-7206	7200-CM1	A1
		DES-7210	7200-CM2	A1

Firmware Version	Supported Line Cards				
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		

Upgrading Instructions:

D-Link switches supports firmware upgrading via TFTP server. You may download the firmware from D-Link web site http://tsd.dlink.com.tw and put the download firmware to TFTP server directory path. Please make sure the TFTP server is connected to the switch via RJ45 cable.

Connect a work station to the switch console port and run terminal emulation program capable of emulating 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 a user name and a password. Upon the initial connection, there is no user name or password.

You may use the command **ls** to check the flash usage of chassis system ensuring the space is enough for install package upload or check if the install package had been downloaded correctly to the flash.

To upgrade the switch firmware, execute the following commands:

Command	Function
`copy tftp://<tftp server ip>/<server file name> flash:firmware.bin`	Copy the specified file from the URL on the host to the equipment.
`ls`	Display the file name of current boot image and configuration.
`redundancy forceswitch`	Switchover the role of master and slave CM
`reload`	Reset the switch.

Upgrade the Chassis with Single Control Module

After rebooting the device with the new firmware, system will synchronize line card firmware automatically once it detects line cards with different firmware version.

Example:
```
Switch#copy tftp://192.168.217.230/firmware for CMII.bin flash:firmware.bin

Transmission finished, file length 21418752

DES-7210#reload
Processed with reload? [no]y

Installation process finished successfully ...
HAL-5-SYS RESTART: System restarting, for reason 'Upgrade product !'.

System bootstrap ...
Nor Flash ID: 0x00010049, SIZE: 2097152Byte
Press Ctrl+B to enter Boot Menu ......

Card in slot [4] need to do version synchronization ...Current software version :
BOOT VERSION: 10.2.37970
CTRL VERSION: 10.2.37970
MAIN VERSION: 10.2.37970
Need update to software version :
BOOT VERSION: 10.3.41188
CTRL VERSION: 10.3.41188
MAIN VERSION: 10.3.41188
Install package transmission begin, wait please ...
Transmitting install package file to slot [4] ...
Transmitting file install lc 20070010.bin;
Transmitting install package file to slot [4] OK ...
Install package transmission finished, system will reset cards ...

AUTO UPGRADE-6-VER SYNC SUCCEED: Version synchronization for card in slot [4] is
OK.

DES-7210#
```

Upgrade the Chassis with Dual Control Module

Upgrade the chassis firmware version v10.3(3b12) or earlier

The firmware v10.3(3b12) or earlier version cannot synchronize the image of master CM and slave CM, administrator have to manual download the firmware to two CM individually. Please follow the steps below to upgrade the chassis.

1. Download the Install Package to the Master CM

Example:

```
Switch#copy tftp://192.168.217.230/firmware for CMII.bin flash:firmware.bin

Transmission finished, file length 21418752。

Switch#redundancy forceswitch
Proceed with switchover to standby PRE? [N/y]y
System bootstrap ...
Nor Flash ID: 0x00010049, SIZE: 2097152Byte
Press Ctrl+B to enter Boot Menu ......
```

Download the Install Package to the Slave CM

After switchover, on obtaining the restart information of the current slave CM, you should connect the RJ-45 cable to the current master CM.

⚡ Warning

It takes about 4 minutes to implement the CM switchover. You shall download the intall package and reset the current master CM before printing the following information:

```
Installation process finished successfully ...
HAL-5-SYS_RESTART: System restarting, for reason 'Upgrade product !'.
```

---

2. Execute the following steps to upgrade the current master CM
Then, you can download the install package using the following command:
DES-7210#**copy tftp**://tftp_server_ip/server_file_name **flash**:**firmware.bin**
tftp_server_ip：IP address（It must be in the same IP segment with the switch）
server_file_name：file name（Upgrade file name in the PC）
For example:
DES-7210#**copy tftp**://*192.168.217.230/firmware_for_CMII.bin* **flash:firmware.bin**
Next, you can reset the switch and upgrade using command **reload**.
DES-7210#**reload**
It prompts:
Installation process finished successfully ...
HAL-5-SYS_RESTART: System restarting, for reason 'Upgrade product !'.
Then note the time and connect the RJ-45 cable to the current slave CM.

Auto-sync
The master CM checks the firmware information of every linecard. If the versions of the linecard and the master CM are inconsistent, auto-sync begins. It prompts:

```
Card in slot [4] need to do version synchronization ...Current software version :
BOOT VERSION: 10.2.37970
CTRL VERSION: 10.2.37970
MAIN VERSION: 10.2.37970
Need update to software version :
BOOT VERSION: 10.3.41188
CTRL VERSION: 10.3.41188
MAIN VERSION: 10.3.41188
```

Then, the master CM will transmit the corresponding install package to the linecard. It prompts:

```
Install package transmission begin, wait please ...
```

```
Transmitting install package file to slot [4] ...
Transmitting file install lc 20070010.bin;
System warmstart.
Transmitting install package file to slot [4] OK ...
Install package transmission finished, system will reset cards ...
```
Next, the linecard resets and upgrades. After a few minutes, linecard upgrade is successful and it prompts:
```
AUTO UPGRADE-6-VER SYNC SUCCEED: Version synchronization for card in slot [4] is
OK.
```
Hence, The whole upgrade is implemented. You can check using command **show version**.
Firmware Upgrade for v10.3(3b12) and later
For the firmware in v10.3.00(3b12) and later, the Master CM can auto-synchronize the slave CM, it prompts:
```
Upgrade file to Module(s) in slot: [4]
Please wait……
Upgrade file to Module in slot [4] OK!
```
So you can skip step 8.2.1.2-8.2.1.4 and reload the switch.
You may follow the steps below to upgrade:
1. Download the install package to the master CM using command copy tftp.
2. Reset the switch using command reload after successful download and the switch synchronizes the slave CM and the linecard automatically.
Check the firmware after upgrade using command **show version**.

New Features:

Firmware Version	New Features
v10.3(5)	1. Support the dynamic LACP function.
v10.3(3b19)	1. Configurable VLAN ID changes from 1-4093 to 1-4094 2. Selective Q in Q 3. Root Guard 4. Loop Guard 5. Supports the MSTP interconnection with the Cisco Catalyst 3550 12.2(25)SEC or later). Flow-based and one-to-many port mirroring. 6. RSPAN 7. Dynamic VLAN assignment for 802.1X after successful authentication. 8. Identity Driven ACL for 802.1X 9. TACACS+ for Management Access 10. VLAN-based ACL for Enhanced I/O Module 11. IP Source Guard. 12. Supports the MPLS(L3 VPN), which requires 7200-ASE3. 13. VRF: VRF-aware DHCP VRF-aware SNMP VRF-aware Syslog VRF-aware AAA VRF-aware TACACS+ 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. Alias option for command line. 6. Include/exclude option for show commands. 7. Support link state check for LACP member ports 8. Auto Edge Port function for MSTP 9. PIM Snooping 10. 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 Command Line Interface:

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

Firmware Version	Changes
v10.3(5)	None
v10.3(3b19)	None
v10.2(2)	None
v10.1(4)	First release

Problem Fixed:

Fixed Revision	Problem
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 can not 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 number 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 swith 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:

  Ruijie(config)#service dhcp;

- Enable the option dot1x function:

  Ruijie(config)#ip dhcp relay information option dot1x;

- Enable the dot1x authentication function on the switch port:

  Ruijie(config)#interface gigabitEthernet 0/1

  Ruijie(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

v10.3(5)	1. 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.
	
	 100 OSPF routes could be forwarded using command clear ip ospf pro. Layers could be consistent using command ip ref synchronize all.
	
	 2. Only the ports on 7200-24GE could be used as the intermediate switch port to apply RSPAN feature.
	
	 3. One RSPAN destination port can only belong to one session.
	
	 4. When enabling PIM and IGMP SNOOPING at the same time, 2 problems below occur:
	   ● PIM and IGMP SNOOPING SVGL mode cannot coexist.
	   ● PIM and IGMP SNOOPING Source IP check can not coexist.
	
	 5. You could create N routed ports and 4094-N VLANs. The system prompts the VLAN creation error if a routed port has occupied the VLAN. That is to say, on condition that the idle VLANs are in the system,
	   ● Each routed port requires 1 idle VLAN;
	   ● Each Layer-3 AP requires 1 idle VLAN;
	   ● Executing label-switching command once or for multiple times consumes 1 idle

VLAN;

- Creating 1 VLAN requires 1 idle VLAN;
- 4094 idle VLANs are in the system in all.

6. The amount of L2 and L3 multicast entries must be equal to or less than 1000 since the maximum limit for the hardware multicast entries is 1000.

Entries could be created on both L2 and L3 when L2 and L3 multicast coexist:

- (*,G,v) are created and entries are consumed on conditon that the multicast flow or VOD exist in the VLAN with IGMP SNOOPING enabled;
- (s,g,v) with output vlan_1,vlan _2... vlan_n are created on condition that the L3 multicast is enabled.

If a multicast sends N data flow and VOD is able to receive them, N (*,G,v) on VOD input will be created, and L3 multicast will create N (s,g,v). N*M (*,g,v) entries will be created if L3 multicast have M SVI output. Therefore, the entries are N+N+N*M in total.

You could get the L3 multicast amount using command 'show ip mroute count' , and the total multicast entry amount which contains L2 and L3 multicast entry using command show msf.

Large amount of entries would be consumed with L2 and L3 multicast enabled. You shall disable L2 multicast in the VLAN without SNOOPING to release the entries.

7. Unsupported items for 7200-24GE and Secure ACL are listed as follows:

- ACL 80;
- Extended IP ACLs: ICMP(Protocol Type);
- Extended IP ACLs: Multiple ACE(TCP)TCP attribute fields, for example, port-matching;
- Extended IPV6 ACLs: Matches dIp sPort dPort dscp and flow-label;
- Extended UDPv6 port field;
- Extended UDPv6 dscp and flow-label;
- Extended TCPv6 port field;
- Extended ICMPv6;
- Time-based Expert ACLs;
- Extended IP ACLs: Dscp field;
- Extended IP ACLs: Multiple ACE(IP)fragments attribute fields;
- Mac Extended ACLs: COS shall be applied to the output.

8. 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.

Related Documentation:

DGS-7200 User Manual v10.3(5)
DGS-7200 CLI Manual v10.3(5)
DES-7200 Hardware Installation Guide v1.4