Firmware Version: 2.00.B033
Prom Code Version: v1.00.B007
Published: Jun 09, 2009

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: v2.00.B033 Prom: v1.00.B007	08-June-09	DES-3528	A1, A2
		DES-3528DC	A1
		DES-3528P	A1
		DES-3552	A1
Runtime: v1.03.B013 Prom: v1.00.B007	20-Mar-09	DES-3528	A1, A2
		DES-3528DC	A1
		DES-3528P	A1
		DES-3552	A1
Runtime: v1.01B035 Prom: 1.00.B006	18-Aug-08	DES-3528	A1, A2
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. 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.

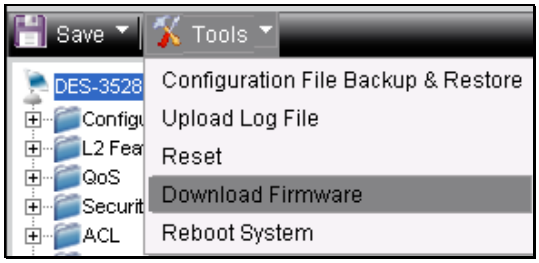
config firmware image_id <1-2> [delete | boot_up]	Change the boot up image file.
show firmware_information	Display the information of current boot image and configuration.
reboot	Reboot the switch.

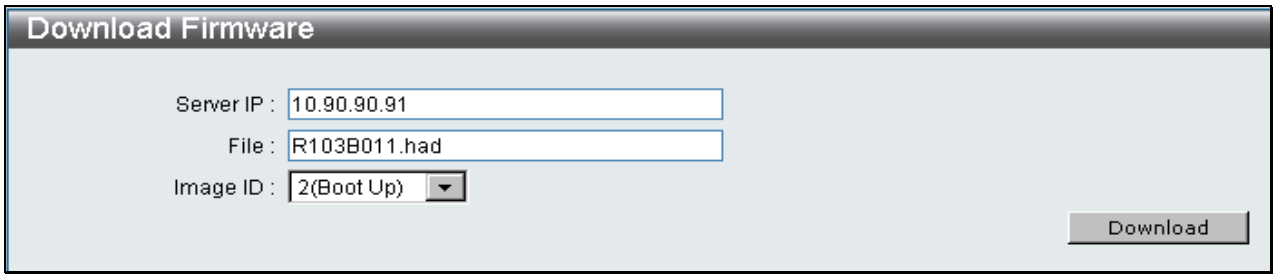
Example:

```
1.  DES-3528:5#download firmware_fromTFTP 10.90.90.91 R103B011.had image_id 2
    Command: download firmware_fromTFTP 10.90.90.91 R103B011.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  1.03.B011 2450452 2009/03/05 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 V1.03.B011 Runtime image ............. 100 %
  UART init .....................
  Device Discovery ......................................... 100 %
  Configuration init ....................................... 100 %
```

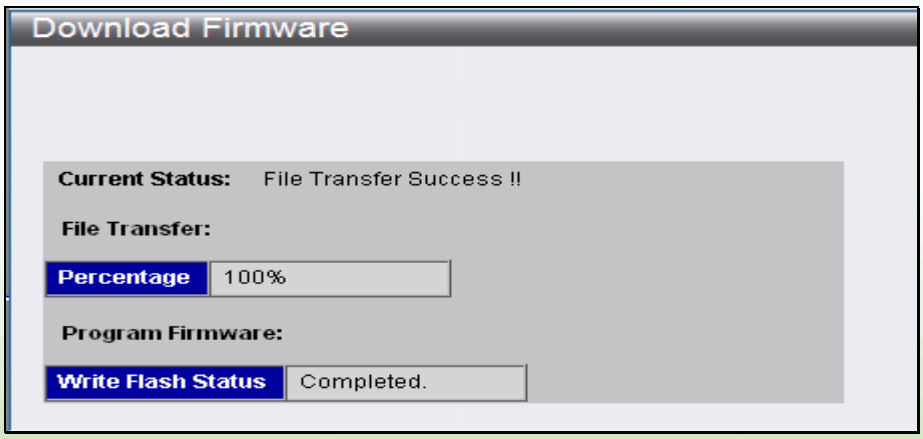
Upgrade using Web-UI

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
V2.00.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. 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. Proxy ARP
19. SNMP trap and system log support for Gratuitous ARP events
20. Configurable default 802.1p priority on each port.
21. Scheduling mechanisms (strict or WRR) can be configured on a per port basis.
22. Per flow bandwidth control can be based on the assigned CoS queue.
23. ACL function supports up to 14 profiles and 1792 rules per system
24. VLAN-based ACL
25. Allows the configuration of SSH port to any desired port number
26. Broadcast/Multicast Storm Control allows the configuration of 5 minutes recovery timer for shutdown ports
27. IMPB V3.5
    - Configurable threshold number for illegitimate entries that can be recorded in the FDB
28. 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
29. 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
30. 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
31. 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
32. MAC filtering via FDB
33. L3 Control Packet Filtering: Support the filtering of DVMRP, PIM, IGMP Query, OSPF, RIP, or VRRP packets.

	34. Multiple Authentication 35. Authentication database failover: Be able to switch to local database for authentication when RADIUS server fails. 36. Remove the display of MAC address information from "show log" switch command 37. Telnet Client 38. Trusted host that supports up to 10 IP addresses or subnet entries in total 39. SYSLOG ● Support WAC/MAC event logging ● Support storm control block mode logging ● Support spoofing attack logging with IP, MAC address and corresponding port information 40. sFlow support 41. DHCP relay option 60, 61 42. DHCP relay option 82 with group ID support 43. DHCP Server enhancement: Support DHCP server configuration via Web GUI & SNMP 44. Add user IP information in admin ID/password change event logging 45. DNS Relay support 46. Send trap and log when the switch temperature goes over 80 Degrees or downs under 75 Degrees 47. ARP Spoofing Attack Prevention 48. Show product serial number on Web GUI and CLI 49. Add BPDU Attack Protection supports in WEB and MIB 50. 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
V2.00.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	1. 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	1. Add BPDU Attack Protection supports in WEB and MIB
	CableDiag.mib	1. 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	1. Support DHCP Server feature
	Equipment.mib	1. Support the sending of trap and log when the switch temperature goes over 80 Degrees or downs under 75 Degrees
	Filtering.mib	1. 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	1. 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 4. Support Local Authorization feature that accepts the assignment of VLAN value from local database after successful authentication with local database
	l2mgmtDES3528.mib, l2mgmtDES3528dc.mib, l2mgmtDES3528p.mib, l2mgmtDES3552.mib	1. 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	1. Use McastSnooping.mib and McastVLAN.mib to replace the multicast features from L2mgmt.mib
	PoE.mib	1. Support Time-based PoE feature
	QinQ.mib	1. 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	1. Support RSPAN feature
	sFlow.mib	1. Support sFlow feature
	SSH.mib	1. Support the configuration of SSH port to any desired port number
	SubnetVLAN.mib	1. Support subnet-based VLAN feature
	VoiceVLAN.mib	1. Support Voice VLAN feature
	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	1. Add MSTP conformance to IEEE 802.1Q-2005 standard
v1.03.B013	HCNUM-TC.mib; RFC 1850.mib	1. Add HCNUM-TC.mib and RFC 1850.mib for loading L3mgmt.mib
	ie8023ah.mib	1. Support 802.3ah OAM feature
	RFC4188.mib	1. Use RFC4188.mib to replace RFC1493.mib
	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.

Firmware Version	Changes
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
V2.00.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	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
V2.00.B033	1. The web interface does not support user logout and automatic logout when using Apple's Safari web browser. 2. The web interface will generate error message when configuring CFM loopback function through it. However it is working fine when configuring using CLI.	None
v1.03.B013	DES-3552 has following known issues due to chipset limitation: 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	No new Known Issues.	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