



FW Version: 4.3.0.3_B201

Published Date: 2014-09-26

Copyright © 2014

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

Content:

REVISION HISTORY AND SYSTEM REQUIREMENT:	2
IMPORTANT NOTES:	2
NOTES FOR CONFIGURATION AUTO-BACKUP/RESTORE IN USB STORAGE:	2
UPGRADING INSTRUCTIONS:	3
UPGRADING BY USING WEB-UI	3
NEW FEATURES:	3
PROBLEMS FIXED:	3
KNOWN ISSUES:	6
RELATED DOCUMENTATION:	7

Revision History and System Requirement:

Firmware Version	Date	Model Hardware	History
4.3.0.3_B201	26 Sept 2014	DWC-2000/A1	1. Bug fix
4.3.0.3	21 Aug 2014	DWC-2000/A1	1. Bug fix
4.3.0.2_B003	17 Jul 2014	DWC-2000/A1	1. Security Vulnerability Addressed OpenSSL vulnerability (CVE-2014-0224)

Firmware Details:

Image Version	HW	MD5 Checksum
DWC-2000_A1_FW_4.3.0.3_B201_WW	A1	a4859f60a69bb68bff783a5cbd92c208

Important Notes:

1. GNU/Linux Bash Shell vulnerability (CVE-2014-6271)

We have evaluated this vulnerability. DWC-1000 and DWC-2000 are **not** vulnerable to this since these devices do not expose the shell interface through CLI nor WEB interface (including CGI).

Reference website:

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271>

<http://seclists.org/oss-sec/2014/q3/650>

<https://blogs.akamai.com/2014/09/environment-bashing.html>

Notes for Configuration Auto-Backup/Restore in USB Storage:

D-Link DWC Unified Controller support configuration backup or restore automatically while a USB drive is inserted. Following information instructs what condition will perform backup/restore.

1. The configuration will be automatically backed up to the USB drive as soon as the USB drive is inserted. The back name has format <Model Name>_<Serial Number>.cfg provided this USB drive doesn't have a backup configuration file from a DWC already present.
2. The system LED on the DWC blinks 3X in amber to indicate a backup operation has started.
3. The configuration in the USB drive can be updated if the user manually clicks 'Save Settings' in any GUI page and provided the Model Number and the Serial Number of the DWC matches with the file already present in the USB drive.
4. In case of reboot, the DWC checks for the presence of configuration file (with format

ModelName_SerialNumber.cfg). If found, the configuration from the USB drive is restored on the DWC. If a configuration file with the correct format is present in both connected USB drives, the configuration from the first USB drive will be used to restore the DWC.

5. The USB drive can have only one configuration with the above mentioned format for each model name.
6. If the USB drive is plugged in to the DWC which is in factory default state, then during reboot, no backup is taken since no custom configuration file exists in the DWC by that time. The custom configuration is stored on the USB drive once the user clicks Save Settings in any GUI page.

Upgrading Instructions:

Upgrading by using Web-UI

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the *DWC-2000 User Manual ver. 1.00*.

New Features:

Firmware Version	New Features
4.3.0.3_B201	RF Scheduler
4.3.0.3	N/A
4.3.0.2_B003	N/A

Problems Fixed:

Firmware Version	Problems Fixed
4.3.0.3_B201	<ol style="list-style-type: none"> 1. Network freeze issue <ol style="list-style-type: none"> a. Using Smartbit, forwarding packets with 64Bytes/1G/100%, the sample will crash or reboot in few minutes. b. Using IXIA with RFC 2544 (packet size 64 byte and use IP header, no UDP and TCP header), and 1G/sec to send traffic, DWC-2000 will reboot immediately. 2. Cannot configure 802.11ac mode 3. [DBG14040524][DBG14040525][DBG14050115] DWC-2000 should be able to handle more than 64 APs with appropriate license 4. [DBG14060133] Cannot display other LANs information

	<ol style="list-style-type: none"> 5. [DBG14060116] In the web page of Discovered AP List, it cannot display the information more than 100 AP entries. 6. [DBG14060173] Failed to copy the AP profile 7. [DBG14070166] NB can't get IP address after change VLAN interface
<p>4.3.0.3</p>	<ol style="list-style-type: none"> 1. [DBG14060159] The function of select-All is not work as expectation. 2. [DBG14060160] Channel bandwidth selection, Basic rate, support rate, auto eligible channel not work (use case woks only issue with the GUI - low priority for now) 3. [DBG14070263] Critical error pop up on peer managed page under cluster topology. 4. [DBG14070261] Peer controller pager showed incorrect device number on WEB GUI under cluster topology. 5. [DBG14070078] The device shall refuse user to import over-spec number of license. 6. [DBG14070166] NB can't get IP address after change VLAN interface 7. [DBG14070085] With default built-in license, DUT cannot create over 64 APs entries in valid AP database 8. [DBG14070089] The DHCP server available lease time is different between LAN-settings and VLAN-settings 9. [DBG14070109] The RA feature shall not be able to disable while the DHCPv6 stateless mode is enabled. 10. [DBG14070093] DNS host name mapping shall automatically transfer the uppercase character. (works as per RFC but we DSR behavior was requested). 11. [DBG14070107] The feature of "Radius Use Network" is not available on DWC-2000, thus it will cause problem if we turn the feature "on", need to remove this item from the menu 12. [DBG14070083] The feature of Session timeout is not work. 13. [DBG14060564] DWC-2000 doesn't send Radius-request message to radius server while running the WPA2-enterprise on 2.4Ghz radio, note that, 5Ghz radio is work without problem 14. [DBG14060167] The incorrect behavior as setup radio "Mode" (use case woks only issue with the GUI - low priority for now) 15. [DBG14070260] Discover AP pager has pop up critical error under cluster topology 16. [DBG14070102] The managed APs location information will be incorrectly overwritten.

	<p>17. Sync DWS-4026 Auto Channel Algorithm Patch at 5GHz Issue (DI20140507000005) (The same patch in DWC-1000/v4302, SPR #44243)</p>
<p>4.3.0.2_B003</p>	<p>1. Security Vulnerabilities Addressed: Null byte injection attack in URL. Reference: http://www.ultsec.com/null-byte-attack.php Solution: Avoid parsing the null byte in URL and send back that requested URL is not there.</p> <p>2. Vulnerability reported by DEU (nu11.nu11@yahoo.com 2013-08-18) Network access to the router ports 443 and 23. Security Vulnerabilities Addressed: Devices respond clients some unnecessary information, and hence give hackers a chance to get a non-persistent root shell. Reference: CVE-2013-5945, CVE-2013-5946 http://packetstormsecurity.com/files/124319/D-Link-DSR-Router-Remote-Root-Shell-Overview.html http://dl.packetstormsecurity.net/1312-advisories/dlinkdsrrouter-writeup.txt http://web.nvd.nist.gov/view/vuln/search-results?query=Dlink&search_type=all&cves=on Solution: Remove all unnecessary root user account</p> <p>3. OpenSSL CCS Injection vulnerability (man-in-the-middle attack) Security Vulnerabilities Addressed: OpenSSL before 0.9.8za, which allows man-in-the-middle attack, and consequently hijack sessions or obtain sensitive information. Reference: CVE-2014-0224 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224 https://www.openssl.org/news/secadv_20140605.txt Solution: Update OpenSSL patch to 0.9.8za that addresses the vulnerability.</p> <p>4. [DBG14050115] The Web UI presented critical error when managed the maximum supporting number of APs (256 APs)</p> <p>5. [DBG14070098] DUT shall not answer the ARP request traffic from different VLAN.</p> <p>6. [DBG14040541] Device will display failed web page after saving the configuration of remote management.</p> <p>7. [DBG14060564] DWC-2000 doesn't send Radius-request message to radius server while running the WPA2-enterprise on 2.4Ghz radio, note</p>

	<p>that, 5Ghz radio is work without problem.</p> <p>8. [DBG14060122] The session timeout problem.</p>
--	---

Known Issues:

Firmware Version	Known Issues
4.3.0.3	<ol style="list-style-type: none"> 1. [39795] User not able to open and access the Wireless Deployment map page 2. [42610] Unable to push the SLA configuration from cluster controller to peer controller 3. [42629] Billing profile when created for basic limit by usage/duration is getting expired by considering the expiration date & time set from Payment gateway window. 4. [42961] Flow-based Control QOS is not working 5. [43770] Intermittent clustering issue in DWC-2000. 6. [45950] Select all + Delete is not working correctly for AP provisioning page (all items are not being deleted)
4.3.0.2_B003	<ol style="list-style-type: none"> 1. [DBG14060159] The function of select-All is not work as expectation. 2. [DBG14070078] The device shall refuse user to import over-spec number of license. 3. [DBG14070085] With default built-in license, DUT cannot create over 64 APs entries in valid AP database 4. [DBG14070089] The DHCP server available lease time is different between LAN-settings and VLAN-settings 5. [DBG14070093] DNS host name mapping shall automatically transfer the uppercase character. (works as per RFC but we DSR behavior was requested). 6. [DBG14070109] The RA feature shall not be able to disable while the DHCPv6 stateless mode is enabled. 7. [DBG14060167] The incorrect behavior as setup radio "Mode" (use case woks only issue with the GUI - low priority for now) 8. [DBG14060160] Channel bandwidth selection, Basic rate, support rate, auto eligible channel not work (use case woks only issue with the GUI - low priority for now) 9. [DBG14070166] NB can't get IP address after change VLAN interface

Related Documentation:

- DWC-2000 User Manual ver.1.00
- DWC-2000 CLI Reference Guide ver. 1.00