Firmware Version: 3.0.0.12
Published: Jan 14, 2011

Content:

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
Runtime: V3.0.0.12	14-Jan-11	DWS-3026	A1G, A2G, A3G
		DWS-3024	A1G, A2G, A3G
		DWS-3024L	A1G, A2G
Runtime: V2.2.0.22	20-Dec-09	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
		DWS-3024L	A1G
Runtime: V2.2.0.17	20-July-09	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
		DWS-3024L	A1G
Runtime: V2.2.0.15	06-July-09	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
		DWS-3024L	A1G
Runtime: V2.2.0.12	20-Feb-09	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
		DWS-3024L	A1G
Runtime: V2.2.0.4	30-Oct-08	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
		DWS-3024L	A1G
Runtime: V2.1.0.10	30-April-08	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
		DWS-3024L	A1G
Runtime: V2.1.0.9	19-Feb-08	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
Runtime: V2.0.0.6	30-Sept-07	DWS-3026	A1G, A2G
		DWS-3024	A1G, A2G
Runtime: V1.0.2.3.	14-May-07	DWS-3026	A1G
		DWS-3024	A1G
Runtime: V1.0.1.5	27-Oct-06	DWS-3026	A1G
		DWS-3024	A1G
Runtime: V1.0.0.5	16-Aug-06	DWS-3024	A1G

New Features:

Firmware Version	New Features
V3.0.0.12	1. Voice VLAN support: Enables the switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. It safeguards the audio quality of an IP phone from deteriorating when the data traffic on the port is high. 2. RIPv2 support: Supports dynamic routing in the form of Routing Information Protocol version 2. 3. Switch Date/Time Setting: The administrator can set the current date/time on the switch that has a real-time clock support through the Web UI now. 4. SNTP Enhancements: The SNTP client on the switch now has the ability to display the time zone and support daylight saving time. 5. Display Available NVRAM (Flash) Size: The “show nvram-size” CLI command

has been added to display the NVRAM size information.

6. Default SSL Certificate support for access the switch via HTTPS: A default SSL certificate is present on the switch file system so that the administrator can enable HTTPS and access the switch using HTTPS.
7. Null User Authentication: The null user authentication is allowed the administrator login the switch Web UI and serial console by using blank username and blank password.
8. Captive Portal Enhancement
   - Custom Background: The administrator can optionally specify the background image to be used for the client authentication screen on the user's browser window.
   - Client Authentication Logout Request: The administrator can optionally configure and enable 'user logout'. This feature allows the authenticated client to deauthenticate from the network.
   - Captive Portal Default Session Timeout: The default value of the range of Session Timeout is changed from 0 to 86400 seconds.
9. Support DWL-8600AP management: The supported AP hardware types are DWL-3500AP, DWL-8500AP, and DWL-8600AP now.
10. AP Code Download Enhancements: previous design uses the same code image on both DWL-3500/8500AP. The DWL-8600AP cannot use the same code image as the DWL-x500APs. Therefore the code download application and user interface are enhanced to enable the administrator to specify a different download file for the DWL-3500/8500/8600AP. The administrator can specify two image files, two image paths, and select which image type to download.
11. Channel Assignment Enhancements: The channel selection is enhanced to support 802.11n mode (Only the DWL-8600AP supports 802.11n).
12. AP Profile Enhancements: The radio web page in the profile configuration is enhanced with several new options for 802.11n.
13. AP Hardware and AP Profile Compatibility: The software checks whether APs discovered by the switch are compatible with the profile assigned to them.
14. Enlarge Default SSID values from 8 to 16: The default values of the 16 SSIDs for each radio on any configuration profile are dlink1-dlink16. Note that for a managed DWL-x500AP, only the first 8 SSIDs are sent to the AP as those AP radios support 8 VAPs. For the DWL-8600AP radios, all 16 SSIDs are sent.
15. WLAN Visualization Inactivity Timer: If there is a period of inactivity on the WLAN Visualization applet long enough to let the session expire, a message box pops up to alert the user and to request to re-authenticate the web session via web browser.
16. NetBIOS Name Snooping: If a Windows client is associated with a managed DWL-8600AP or DWL-x500APs, the AP snoops the client NetBIOS name and sends it to the switch, and then switch displays the NetBIOS Name of the client on the CLI, Web, and SNMP.
17. Client Name in Local MAC Authentication List: A user-friendly name of up to 32 printable ASCII characters can be assigned to a client entry in the local Client MAC Authentication list.
18. Local AP Database Summary enhancement: On the switch Web UI, the Valid Access Point Summary page has been added to display a summary of the APs in local database and divide into different types. This summary is also displayed by using the show wireless ap database CLI command.
19. Local AP Database Full GUI message: a popup error message is displayed

	when the local AP database is full. The popup message is “The local AP database is full, failed to add a new AP.” 20. Rogue AP Mitigation (supported on DWL-8600AP only): Helps automatically protect the network against rogue APs by sending de-authentication messages to clients by faking the rogue AP MAC address as the source MAC and BSSID of the de-authentication frame, and using the broadcast MAC address as the destination of the de-authentication packet. 21. Client-based Rate Limiting (supported on DWL-8600AP only): This is new for Client QoS design. With external RADIUS, administrator can limit the Max transmission rate on each wireless client. The rate limiting function is good on limiting UDP transmission rate (like video streaming application), but not well on limiting TCP transmission rate. 22. Support secondary RADIUS server for wireless client authentication. 23. RADIUS server Failover support: a secondary or backup RADIUS server can be defined for wireless client authentication. If the primary RADIUS server is not available, the secondary RADIUS server will act as a “failover” server for wireless client authentication. 24. RADIUS server Fail-through support: In WPA/WPA2-Enterprise security, if the authentication is failed at primary RADIUS server, switch can pass wireless client information to secondary or backup RADIUS server for authentication. 25. DWL-8600AP DFS channels support for Japan - W53, W56 are supported for JP in case of standalone DWL-8600 APs. - W53, W56 are supported for JP in case of DWL-8600 APs managed by DWS-4026 switches. - Partial DFS channels (W53) are supported for JP in case of DWL-x500 APs operating in standalone mode, and DWL-x500 APs and DWL-8600 APs managed by DWS-3000 series switch. 26. Allows the range to be set on the RF scan interval from 30-120 to 30-3600 (seconds).
V2.2.0.22	1. Added Brazil country code (BR) 2. Increased maximum client lease number on DHCP server from 256 to 1,024
V2.2.0.17	1. Added detailed upgrade warning message on AP CLI, GUI and Switch GUI
V2.2.0.15	1. Shortened the Captive Portal loading time 2. Can show summary of the local AP database in CLI and Web GUI 3. Add a warning message when AP database is full 4. Added new Country Code for Russia. Russian regulation requires that all channels from 5.35GHz to 5.65GHz be disabled
V2.2.0.12	1. Updated 802.11a regulatory information as well as power output for the following countries: TW - modified the channels to 52,56,60,64,149,153,157,161,165 SG - modified the channels to 36,40,44,48, 52,56,60,64,149, 153, 157, 161, 165 EC - modified the channels to 36,40,44,48, 149, 153, 157, 161, 165 CR - modified the channels to 36,40,44,48, 149, 153, 157, 161, 165 RO - modified the channels to 36, 40, 44, 48 MY - modified the channels to 36, 40, 44, 48 PK - modified the channels to 36, 40, 44, 48 2. Increased memory usage for WLAN visualization function to allow up to 16 jpgs in the applet, instead of 13 before

	3. Previously, the AP page on Switch GUI will automatically refresh every 30 seconds. A new check box has been added at the bottom of the page next to the refresh button to disable the auto-refresh. [HQ20090213000016] 4. Added a warning message "NOTE: Please do not reset the APs when NVRAM update is in progress." on the switch GUI
V2.2.0.4	1. Supports wired Captive Portal – extends the Captive Portal from v2.1.0.9 for WLAN clients to the clients connected to the physical ports on the Wireless Switch 2. Captive Portal Client web UI Customizations – adds new customizable, language-specific web pages for a Captive Portal instance 3. "User Group" RADIUS attribute support for a Captive Portal user in the RADIUS database – User Groups can be associated to a Captive Portal instance via RADIUS 4. Increased Captive Portal Username / Password for local database and RADIUS to 32 characters 5. Provides a note on the Client Stats page that it is not supported for Wired CP
V2.1.0.10	1. Supports new model DWS-3024L, which manages up to 24 Aps
V2.1.0.9	1. Supports Captive Portal 2. Web UI: ACL Summary Web UI Display enhancements – New pages for IP ACL and MAC ACL are added to display Rule Summary 3. Supports Dynamic VLAN Assignment for a wired station. The client can get assigned to the appropriate VLAN that is configured in the RADIUS server 4. Supports Guest VLAN for wired stations 5. Supports Station Isolation for Managed AP 6. Supports Antenna Diversity configurability 7. Web UI: Modified Power Display – the Web UI displays the power fraction in decibels along with the percentage 8. Enhanced client association trap & syslog – following pieces of information are added: SSID, Authentication method (none / static wep / wep_8021x / WAP_personal / WPA_enterprise) 9. Enhanced Ethernet interface parameters/counters- The following new interface status parameters / counters are supported through CLI, Web UI, and SNMP: *Media Type, ARP Type, Total output drops, Ignored frames, Late collisions, Deferred transmissions, Lost carrier / No carrier* 10. Changed the CLI command 'WPA passphrase' to 'WPA key' 11. Disabled W56 channels for Japan 12. Listed all the possible Channel values in the description of MIB object OID:1.3.6.1.4.1.171.10.73.30.1.11.1.6.0 (wsAPRadio1Channel) 13. Changed the refresh timer for 3 Web Pages (All Access Points, Authentication Failed Access Points, RF Scan/Rogue Access points) from 15 seconds to 30 seconds
V2.0.0.6	1. Supports Path MTU Discovery (RFC 1191) 2. Supports Unified AP 3. Web GUI: New design of login page 4. Web GUI: Logout link is added on the top blue bar 5. Web GUI: Allow configuring timeout parameters for HTTP/HTTPS login sessions 6. Web GUI: *WLAN->Administration->AP Management -> Software Download*

	page: - Allow selecting multiple AP for software downloading. (The admin can select either one Managed AP or all the Managed Aps in previous release) - An Abort counter is provided in this page which shows if all the Aps aborted upgrading or none - An activity bar is displayed once the AP NVRAM upgrade is in progress so that the user is aware there is some activity going on 7. Web GUI: *WLAN->Monitoring->Access Point->All Access Points* page: All the columns on this page except the last 3 (Radio, Channel, and Authenticated Clients) will be sortable 8. *WLAN->Monitoring->Access Point->Authentication Failed Access Points* page, *WLAN->Monitoring->Access Point->All Access Points* page and *WLAN->Monitoring->Access Point->Rogue/RF Scan Access Points* page: After the admin selects one or multiple Aps and clicks 'Manage', a new configuration page is shown for configuring the Aps 9. *WLAN->Monitoring->Access Point->Managed Access Points* page and *WLAN->Monitoring->Access Point->All Access Points* page: A 'Switch Port' column will be added to indicate which physical port on the switch the AP is connected to directly or indirectly in the same L3 domain 10. *WLAN->Monitoring->Access Point->Rogue/RF Scan Access Points* page and *WLAN->Monitoring->Access Point->All Access Points* page: A new button named 'UnAcknowledge' is added. It allows the user to 6nacknowledged an already Acknowledged rogue AP without going to the Valid AP page and deleting from there 11. *WLAN-> Administration ->Basic Setup->Valid AP->Valid Access Point Configuration* page: - Allow resetting the AP immediately after changing the parameter of a valid AP without going to the AP Reset page 12. The WLAN Visualization window lists the Managed APs by their IP addresses and not by their MAC addresses
V1.0.2.3	1. Web GUI: Synchronize the color code on all the pages that show Aps: Managed APs: Green Failed or Rogue APs: Red Acknowledged Rogue APs: Gray Peer Managed APs: Amber 2. Web GUI: In WLAN visualization window, modify the dimension name "Height" to "Length" for Selection dropdown box in the Scale Factor section of Edit Graph Definition and New Graph Definition Dialog Box. The field name 'Length' below the dropdown box is changed to 'Size' to avoid confusion 3. Web GUI: Modify the failed AP icon in visualization window 4. Web GUI: When saving configuration is complete, the *Tools->Save Changes* page will display a message to confirm it 5. Web GUI: Modify the word "Reset" to "Reboot" for all the occurrences on the *Tool->Reboot System* page including the text on the page, button text, help page, the page title when it prompts for the save and the buttons on that page 6. Web GUI: Refine the warning message wording on AP software download page 7. Web GUI: D-Link logo image is made linkable with the URL "www.dlink.com.tw", to redirect to each website of OBU

	8. Web GUI: Correct the D-Link logo on some help pages 9. Web GUI: All Access Points page now shows the channel and the 802.11 mode for rogue APs 10. Web GUI: Correct WLAN Visualization->Download Image page's help page
V1.0.1.5	1. Added new model DWS-3026 2. Modified the status message on the AP Software Download page to clarify the downloading and upgrading process
V1.0.0.5	First Release

Problems Fixed:

Firmware Version	Problems Fixed
V3.0.0.12	1. Show the error message "Failed to set CST Configuration/ Status" on Spanning Tree CST Configuration/Status page even the configuration is correct. [DI20100302000011] 2. Editing and changing the graph image repeatedly through the "Edit→Edit Graph menu" on WLAN Visualization Tool might cause the switch reboot automatically. [DI20100407000001] 3. The PoE power budget does not reach 370W. [DUSA20100528000001] 4. After enabling the Captive Portal feature, the management access to the switch or access to the network through the Captive Portal authentication might become unresponsive after a period of several hours or days. The switch must be rebooted to regain management control. [DCA20100210000001][DUSA20100507000002][DI20100209000006][DI20100308000004][DRU20100512000001] 5. After configuring 2 AP profiles (one for DWL-8600AP, and another for DWL-3500AP), the 802.11b/g setting on DWL-3500AP profile will become disabled after rebooting the switch. [DI20100921000001]
V2.2.0.22	1. When a forced Disassociate message was sent from a Switch to its managed AP to disassociate a client, client RADIUS information is still cached in AP so the client does not need to re-authenticate [DCA20090629000001] 2. AP would store RADIUS response time for up to an hour, making clients unable to re-authenticate if they fail MAC authentication using RADIUS during that period [DI20091022000008]
V2.2.0.17	1. In show running config, summertime mode was not checked and was displaying in config even thought it had default values 2. Captive Portal idle timeout didn't work correctly
V2.2.0.15	1. Sometimes RF Scan does not scan other channels 2. The Signal Strength of Rogue AP is not correctly displayed on the web. [DEUR20090407000003]
V2.2.0.12	1. Very rarely, WLAN Utilization goes over 100%. [HQ2009020200002] 2. VLAN Routing did not function correctly
V2.2.0.4	1. Lost ARP Request frame from wired line in DWL-8500AP - When a dynamic VLAN is deleted, the WPA group state machine is left in an unknown state; when the VLAN is recreated, the state machine is never restarted. This caused some ARP Request frames from a wireless client to be dropped 2. Corrected the default values for wsNetworkTunnelStatus and wsTunnelMtu objects 3. When NV image is not completely loaded, user is not prompted with a failure message. This happened to NV images with size bigger than 1MB 4. EAP Auth Fail for DWL-8500AP/DWS-3026 - There was no check for the dynamic VLAN counter at the MIN value. Therefore, after 0, INT is decremented further to show up as 65,535 and so on, failing the dynamic VLAN MAX check 5. Previously CLI did not prevent associating with more than one Captive Portal configuration 6. CLI also did not allow assigning a group to a Captive Portal configuration with

	RADIUS verification mode 7. After switch rebooted, the Captive Portal interface remained in disabled state, causing all wired & wireless clients to not re-authenticate correctly when using static IP 8. After upgrade from 2.1 to 2.2 for a switch with static IP, the associated wireless interface comes up disabled
V2.1.0.10	1. If DWL-8500AP is operating with its 802.11a radio turned on in a country that requires radar detection for 802.11a channel selection (eg. GB, JP), sometimes the AP incorrectly becomes unmanaged 2. Correct the SNMP MIB description of OID:1.3.6.1.4.1.171.10.73.30.1.11.1.7.0(wsAPRadio2Channel) OID:1.3.6.1.4.1.171.10.73.30.1.11.1.6.0(wsAPRadio1Channel) 3. Help information of Captive Portal trap is not available
V2.1.0.9	1. After upgrading to 2.0.0.x from 1.0.2.3 from IE browser, web pages show small compact tables rather than right-frame wide tables. This does not happen if the switch is upgraded through the CLI 2. The APs become "Connection Failed Access Points" occasionally 3. Wireless clients cannot access AP after the AP starts up for several days 4. A large ping packet to the L3 tunnel will be dropped 5. Admin cannot input a WPA key longer than 32 characters 6. Admin cannot connect to the Web UI after a few days of run 7. After SSH idle timeout, the switch hangs up 8. Switch stops responding to SSL from APs after a few days of run, and then cannot manage APs 9. The help screen of copy command on CLI has an extra '<' character 10. Serial Number on the CLI and Web GUI is not displayed correctly
V2.0.0.6	1. POE related configuration on the switch does not get preserved across resets 2. Sometimes, when a new client associates with the AP, the switch displays a 'roam' trap message 3. The IP 0.0.0.0 can be added in Radius Accounting Server setting page and cannot be deleted 4. The LED of port 2 & 3 flash amber when the active links go beyond 14 ports 5. Web GUI does not incorporate with Java Runtime v1.6
V1.0.2.3	1. Fixed the issue that the results from some OID values (APMacAddress, OID: 1.3.6.1.4.1.171.10.73.30.1.11.1.1, ManagedAPMacAddress, OID: 1.3.6.1.4.1.171.10.73.30.8.1.1.1) were incorrect
V1.0.1.5	1. In Sentry mode the AP scans all channels independent of the switch profile configuration 2. The Web page for VAP does not always update properly 3. When changing to a particular Country Code the available channels for the A-band is not listed correctly in the drop-down menu on the web page 4. The Power Save mode does not work correctly 5. The VAP status is setting more than one VAP when using SNMP
V1.0.0.5	None

Known Issues:

Firmware Version	Issues
V3.0.0.12	1. WLAN Visualization feature only supports IE6 or IE7 now. It might not work correctly with Internet Explorer 8. 2. When WPA/WPA2-Enterprise security is enabled, first-time roams between x500 APs and 8600 APs may require a new session to be established from the RADIUS server. The PMK exchanges between the x500 and 8600 APs failed due to the different size and structure of the PMK data on the x500 and 8600 APs. So the first time a client roams between the x500 and 8600 APs is not fast roaming, but subsequent roams support fast roaming. 3. The download and upload speeds do not fit the values defined in the Client QoS Bandwidth Limit settings on TCP packets. The observed values are much higher than the defined ones.
V2.2.0.22 V2.2.0.17 V2.2.0.15 V2.2.0.12 V2.2.0.4 V2.1.0.10	1. A switch with firmware v2.1.0.x may have problem detecting APs with firmware v1.0.x.x. When upgrading from v1.0.x.x to v2.1.0.x, be sure you upgrade APs first, then upgrade the switch (A v1.0.x.x switch can detect v2.1.0.x APs) 2. Using TKIP/RC4 encryption with WPA2 results in roughly 30% lower throughput than using AES encryption due to a hardware limitation 3. Turbo/SuperG mode does not increase traffic rate significantly 4. Filename with a space character is not supported for Visualization image 5. When the country code is changed on the wireless switch, it is recommended that the user reset the switch after saving the configuration. Failure to reset the switch may result in inconsistent operation 6. Tunneling is not expected to work with port-based routing interfaces. All tunneled routing interfaces must be VLAN routing interfaces. APs should not be attached to the switch via port-based routing interfaces as well 7. More than 1024 characters cannot be added to the AUP (Acceptance User Policy) for CP Web Customization 8. If a captive portal instance is associated with a disabled VAP, re-enabling the VAP does not automatically enable the captive portal instance
V2.1.0.9	1. If DWL-8500AP is operating with its 802.11a radio turned on in a country that requires radar detection for 802.11a channel selection (eg. GB, JP), sometimes the AP incorrectly becomes unmanaged. V.1.0.10 fixed this problem
V2.0.0.6	1. A switch with firmware v2.0.0.6 may have problem cooperating with an AP with firmware v1.0.2.6 or below. Be sure the switch and the AP are both upgraded to v2.0.0.6. (Only DWL-8500AP supports v2.0.0.6. DWL-3500AP does not support v2.0.0.6 at this moment. In an environment with DWL-3500AP, it is suggested to use v1.0.2.3 firmware for the switch
V1.0.2.3 V1.0.1.5 V1.0.0.5	None

Related Documentation:

- DWS-3000 Series User Manual

- DWS-3000 Series CLI Manual
- DWL-3500AP & DWL-8500AP & DWL-8600AP Unified AP Guide