Firmware Version: 4.1.0.8
Published: Apr 25, 2012

Content:

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
Runtime: V4.1.0.2	15-Jan-12	DWS-4026	A1G
Runtime: V4.1.0.8	25-Apr-12	DWS-4026	A1G

New Features:

Firmware Version	New Features
V.4.1.0.8	No new features. Bug fix release only.

V4.1.0.2 (Wired)	First V4.0 (internally referred to as Helio2) release. Baseline feature reference V4.0 functional spec
	New Features and changes over V3.0.0.16 include
	● Time zone and daylight saving time support is added for SNTP clients
	● 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 GUI. There is no CLI or SNMP support for this feature
	● SNTP enhancement – The SNTP client on the switch now has the ability to display the time zone (offset from the UTC) and support daylight savings time. Although the negative time zone offset is allowed up to -12 hours, the configuration is not allowed to the negative offset to bring the adjustment time to one earlier than 00:00:00 Jan 1, 1970.
	● Available flash size – The CLI command `show nvram-size` displays the NVRAM size information.
	● Smart fan support – The DWS-4026 switch uses temperature sensor chip LM75 for smart fan support
	● MIB file change – The SNMP MIB files delivered with the switch binary image now have .mib file extension instead of .my extension. The AP's MIB file also have the same extension.
	● Null user authentication – The null user authentication is allowed when the switch's administrator username is admin (case insensitive) and password is blank. The administrator can also login to the switch Web GUI and serial console by using blank username and blank password. The null user has the same privileges as the admin user. The null user authentication is disallowed in the following cases
	  ● When the password of the admin user has been changed to a non-blank password
	  ● When the admin username has been changed to a username other htan admin.
	● Client and AP location tracking and WLAN visualization – The ability to track the location of wireless clients, APs, and rogue APs via a coordinate system or on a floor plan graphic
	● Power over Ethernet – The D-Link POE solution provides power management which supports power reservation, power prioritization, and power limiting. Administrator can assign a priority to each POE port. When the POE switch has less power available with it and more ports are required to supply power, the higher priority ports are given preference to the lower priority ports. Lower priority ports are forcibly stopped to supply power in order to provide power to higher priority ports. The Static Power Management feature allows administrator to reserve a guaranteed amount

	of power for a POE port. This is useful for powering up devices which draw variable amount of power and provide them an assured power range to operate within. In Dynamic Power Management feature, power is not reserved for a given port at any point of time. The power available with the POE switch is calculated by subtracting the instantaneous power drawn by all the ports from the maximum available power. Thus more number of ports can deliver power at the same time. This feature is useful to efficiently power up more number of devices when the available power with the POE switch is limited. The D-Link POE solution also provides usage threshold feature in order to limit the POE switch from reaching an overload condition. The administrator can specify the limit as a percentage of the maximum power. • POE power budget – The POE power budget is set to 370 Watts • Radio resource measurement – The radio resource measurement feature enables the Unified Wireless Solution to provide information to the wireless clients to help them make roaming decisions. The RRM feature also enables the Unified Wireless Solution to gather information from wireless clients. • RADIUS-based dynamic VLAN assignment – Support has been added to dynamically create VLANs in the system if VLANs assigned by RADIUS servers for 802.1x authenticated clients do not exist in the system. This is supported for only VLAN IDs and not RADIUS server assigned names. • IPv6 management – An IPv6 management FLEX package for Routing builds allow all non-routing specific functionality (e.g. ping, traceroute, TFTP, SNMP, etc.) to be available via the servie and network ports via IPv6 networks. This enables dual IPv6/IPv6 operation over the network port. Capabilities usch as static assignment of IPv6 addresses and gateways for the service/network ports, the ability to ping an IPv6 link-local address over the service/network port, as well as SNMP taps and queries via the service/network port, is added.

V4.1.0.2 (Wireless Management)	• The following information elements are added to the existing client association trap (trap and syslog)
	  • SSID to which the client is associated
	  • Authentication method used by the client
	• New client association failure and client authentication failure traps
	  • SSID to which the client is associated
	  • Authentication method used by the client.
	• Local AP database summary – on the switch WebGUI, the summary of the local AP database, in terms of the number of APs of different type, is displayed just above the list of the APs in the database. Similarly, the summary is shown in the CLI by the `show wireless ap database` command.
	• Due to significant software changes between Release 3.x and Rlease 4.x, a DWS-4026 running firmware from one release will not be a ble to manage DWL-8600 APs running firmware from another release. The following procedure is recommended when upgrading switches and APs from Release 3.x firmware (including the AP running Release 3 images) to Release 4.0 firmware.
	• Use the DWS-4026 switch to upgrade all the managed APs to a release 4.0 image
	  1. The switch temporarily loses management of the APs after the APs boot up with the release 4.0 image

2. Upgrade the switch with Release 4.x firmware
3. The switch shall re-manage all the APs after boot up with the Release 4.0 firmware

- RADIUS fail-through and failover

  Secondary or backup RADIUS servers can be defined for wireless client authentication using WPA-Enterprise security. The secondary servers act as fail-through servers. In fail-through behavior, if a user is not authenticated successfully by the primary server, the authentication request is sent to a secondary server after receiving the re-authentication request from the client. If the user is not authenticated successfully by the secondary server, the authentication request is sent to next secondary server after receiving the re-authentication request from the client. The authentication fails if the primary server and all the secondary servers deny the authentication request from the client. Secondary servers also act as „failover" servers in the sense that the authentication requests are sent to the secondary servers if the primary server is not available for some reason

  For a managed AP solution, the secondary servers are defined along with their secret in the AP configuration profile on the DWS-402x switch. Just like the primary RADIUS server, the secondary server configurations are sent to the AP when it becomes managed. When a wireless client tries to authenticate with the AP using RADIUS, the AP uses the primary and secondary solution as described above.

  The Radius primary and secondary servers can be configured in an AP profile at global level as well as at network level. Whether the global Radius servers or the Radius servers configured at network level are to be used is decided by the global-radius flag defined for the network. The configuration of the RADIUS fail-through is supported on the switch via Web UI, CLI, and SNMP

  When Radius fail-through is enabled, a wireless client tries to authenticate with the AP and if the primary server responds with a RADIUS REJECT, the AP sends an EAP failure to the client. The user may be required to re-enter login credentials depending on the client is used. If the client re-authenticates within 60 seconds, the authentication request is sent to the secondary server and so on. If client does not re-authenticate within 60 seconds, the authentication request is sent to the primary server

  1. When fail-through is enabled, in case of the primary or a secondary server sends a reject and the current secondary server responds with ACCESS-ACCEPT, the client is successfully authenticated. The subsequent authentication requests from the client may be sent to the current secondary server directly in the following scenarios: If session-timeout is configured in the RADIUS Server with Termination-action as radius in the RADIUS Server, the AP will send the radius request to the current secondary server after the timeout.

  2. If the client disconnects and reconnects immediately, the request is sent to the primary server if the client reconnects after 30 seconds. If the client connects within 30 seconds the radius request would be sent to the current secondary server.

  When Radius fail-through is disabled, the AP will send an EAP Request Identity to the client after 60 seconds if the primary server responds with a RADIUS REJECT. In current release, the Radius fail-through is not available for Captive Portal client authentication

and Radius based MAC authentication

The concept of fail-through is not applicable to RADIUS accounting. But if accounting is enabled in the AP profile, the secondary servers act as backup servers.

All the APs which operate at the managed and standalone modes support up to 4 RADIUS servers. In this release, these servers are used as fail-through servers

The Radius failover feature is enabled by default for this release and is not to be disabled by the administrators. The Radius fail-through can be enabled or disabled by administrators.

- On the Web UI, the D-Link WLAN System provides counters for authentication failed AP and the number of the 802.11n clients associated with the system. Those could be 802.11a, 802.11a/n, 802.11b/g,802.11b/g/n, or 802.11 2.4GHz n or 802.11 5GHz n clients.
- The managed AP in the combo box on the AP Software Download page is displayed in the <MAC Addr>-<IP Addr>-<Location> format. Location is optional; therefore it is at the end. The other two fields are mandatory for a managed AP.
- For the CLI command on Unscheduled Automatic Power Save Delivery, the D-Link Release 4.0 will continue to use u-apsd on both switch and APs.

Problems Fixed:

Firmware Version	Problems Fixed
V.4.1.0.8	1. Watchdog software reboot after executed 16VAPs throughput tests and re-loaded ap_profile.. [LVL700168237] (Function is as designed. CPU is inadequate to handle high amount of traffic with 16VAPs) 2. Network Visualization, Switch crashes if back ground image of size 3-4Mb is downloaded [LVL700168551] (Size up to 2MB supported) 3. The switch crashes after changes are made to a managed AP, then reloaded the AP.[LVL700168558] 4. Crash while running openload. [LVL700168871] 5. Network Visualization drag & drop functionality does not work with Java SE 6 update 23 (1.6.0_23) and no error given to user. [LVL700169145] 6. RADIUS_MSG_SEND_FAILED with RADIUS AP auth and validation. [LVL700169474] 7. Higher Roaming Delay values of 250msecs seen when Roaming test executed using WPA2-Enterprise. [LVL700171996] 8. Script apply is getting failed due to incorrect saving of hardware type command. [LVL700174693] 9. Captive portal max-bandwidth limit. [LVL700163126] 10. If modified the pmtu setting, the STA is able to access network without CP authentication. [LVL700168249] 11. Incorrectly L2 Tunnel statistics. [LVL700168261] 12. RO user is able to perform read write applications of Network Visualization. [LVL700168632] 13. Network Visualization, Graph is not being updated when a client station is disassociated from MAP. [LVL700168669] (Function is as designed. Client must disassociate and remove from database. 14. Network Mutual Authentication Status says "Complete with Errors" but no indication of what errors are or why they occurred. [LVL700168931] 15. AP Authentication Failure Status shows "AP Relink" but that's not listed as one of the possible reasons on Help page. [LVL700169048] 16. TSPEC-UWS: Roam reserve limit functionality is not working and new AP is not allocating BW for roamed client. [LVL700169279] 17. Doing a push using the GUI takes an excessive amount of time. [LVL700169404] 18. Associated client listed as "Rogue". [LVL700169420]

	19. RADIUS client set to "grant" denied access to VAP. [LVL700169473] (Function is as designed) 20. Peer connection lost when large CP images are loaded. [LVL700169593] 21. When changing AP Profile -> QOS to factory default, Summary tab doesn't show "modified". [LVL700170973] 22. Roaming delay test fails when executed for multiple clients due to failed roams. [LVL700171690] (configuration issue) 23. Spoofed De-auth messages are not seen from managed AP when client is associated to unmanaged AP with same SSID. [LVL700171761] (configuration issue) 24. No syslog msg when max managed AP limit reached on a single UWS and also when the max exceeded for the cluster. [LVL700171884] 25. 802.1X authentication fails. [LVL700171976] 26. After sSelecting multiple AP's for the switch to provision, it only provisions one. [LVL700174565] 27. Failed to push Bandwidth parameters of Client QoS by using Radius attributes. [LVL700175157]Jack
V.4.1.0.2	Initial release

Known Issues:

Firmware Version	Issues
V4.1.0.8	1. Client Security pre-auth history. [LVL700169403] 2. Roaming Delay values are high for WPA2-PSK when test is run in b/g/n band. [LVL700157839] 3. Probe Req Recorded values are not correct. During collection interval they will sometimes decrease. [LVL700169678] 4. Network parameter 'ignore broadcast' is not being set on AP. [LVL700171186] 5. When the max managed number of APs is exceeded the reported failure is "No database entry" when in fact there is an entry. [LVL700171885] (Very difficult to reproduce) 6. Setting "Tagging All" does not actually set Tagging all in VLAN configuration. [LVL700171964] 7. Channel management page shows content for 8 APs, but 11 are clustered. [LVL700172120]
V4.1.0.2	1. Watchdog software reboot after executed 16VAPs throughput tests and re-loaded ap_profile.. [LVL700168237] 2. Network Visualization, Switch crashes if back ground image of size 3-4Mb is downloaded [LVL700168551] 3. The switch crashes after changes are made to a managed AP, then reloaded the AP.[LVL700168558] 4. Crash while running openload. [LVL700168871] 5. Network Visualization drag & drop functionality does not work with Java SE 6 update 23 (1.6.0_23) and no error given to user. [LVL700169145] 6. Client Security pre-auth history. [LVL700169403] 7. RADIUS_MSG_SEND_FAILED with RADIUS AP auth and validation. [LVL700169474] 8. Higher Roaming Delay values of 250msecs seen when Roaming test executed using WPA2-Enterprise. [LVL700171996] 9. Script apply is getting failed due to incorrect saving of hardware type command. [LVL700174693] 10. Roaming Delay values are high for WPA2-PSK when test is run in b/g/n band. [LVL700157839] 11. Captive portal max-bandwidth limit. [LVL700163126] 12. If modified the pmtu setting, the STA is able to access network without CP

authentication. [LVL700168249]

13. Incorrectly L2 Tunnel statistics. [LVL700168261]
14. RO user is able to perform read write applications of Network Visualization. [LVL700168632]
15. Network Visualization, Graph is not being updated when a client station is disassociated from MAP. [LVL700168669]
16. Network Mutual Authentication Status says "Complete with Errors" but no indication of what errors are or why they occurred. [LVL700168931]
17. AP Authentication Failure Status shows "AP Relink" but that's not listed as one of the possible reasons on Help page. [LVL700169048]
18. TSPEC-UWS: Roam reserve limit functionality is not working and new AP is not allocating BW for roamed client. [LVL700169279]
19. Doing a push using the GUI takes an excessive amount of time. [LVL700169404]
20. Associated client listed as "Rogue". [LVL700169420]
21. RADIUS client set to "grant" denied access to VAP. [LVL700169473]
22. Peer connection lost when large CP images are loaded. [LVL700169593]
23. Probe Req Recorded values are not correct. During collection interval they will sometimes decrease. [LVL700169678]
24. When changing AP Profile -> QOS to factory default, Summary tab doesn't show "modified". [LVL700170973]
25. Network parameter 'ignore broadcast' is not being set on AP. [LVL700171186]
26. Roaming delay test fails when executed for multiple clients due to failed roams. [LVL700171690]
27. Spoofed De-auth messages are not seen from managed AP when client is associated to unmanaged AP with same SSID. [LVL700171761]
28. No syslog msg when max managed AP limit reached on a single UWS and also when the max exceeded for the cluster. [LVL700171884]
29. When the max managed number of APs is exceeded the reported failure is "No database entry" when in fact there is an entry. [LVL700171885]
30. Setting "Tagging All" does not actually set Tagging all in VLAN configuration. [LVL700171964]
31. 802.1X authentication fails. [LVL700171976]
32. Channel management page shows content for 8 APs, but 11 are clustered. [LVL700172120]
33. After sSelecting multiple AP's for the switch to provision, it only provisions one. [LVL700174565]

	34. Failed to push Bandwidth parameters of Client QoS by using Radius attributes. [LVL700175157]

Related Documentation:

- DWS-4026 Manual
- DWS-4026 CLI Manual