D-Link®

Wireless AC Services Router Release Notes

Firmware Version: 3.10_WW/RU

Published Date: Jan. 04, 2017

Copyright © 2016

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:

dlink green

Revision History and System Requirement:

Firmware Version	Region	Date	Model	HW Version
3.10	WW/RU	Dec. 04, 2016	DSR-500/1000, DSR-500AC/1000AC	B1, A1
3.07	WW/RU	Nov. 04, 2015	DSR-500AC/1000AC	A1

Important Notes:

1. DSR-500AC/1000AC product doesn't support BGP routing and are not affected by the potential vulnerability that is well known as CVE-2004-0230, the attacker can potentially reset the BGP connection with the device.

2. All DSR routers with WW version are not allowed to install RU firmware image in order to prevent unnecessary misunderstanding for customers.

3. Before plug DWM-152/156 3G USB dongle in DSR-500AC/1000AC, please make sure the SIM Card is not set PIN code.

4. Microsoft Windows XP has some well-known limitation to access USB storage of DSR router, D-Link provides a Registry Script file named: WinXP.reg which can solve limitation of Windows XP environment. Without applying this script file, it cannot copy file from Windows XP to USB storage. (This issue will not happen when copy file from USB storage to Windows XP)

5. For any firmware downgrade situation, i.e. from a newer version to an older one, it will take more time to restart system comparing to firmware upgrade, i.e. from an older version to a newer one. If you MUST execute firmware downgrade for your own reasons, please allow DSR more time to reboot system.

6. To authenticate SSL VPN users through external databases including RADIUS, LDAP, AD and POP3, admin must also need to create user accounts with the same username and password in the local user database.

Notes for Configuration Auto-Backup/Restore in USB Storage

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

1. The router 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 DSR router already present.

2. The system LED on the router 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 router matches with the file already present in the USB drive.

4. In case of reboot, the router checks for the presence of configuration file (with format ModelName_SerialNumber.cfg). If found, the configuration from the USB drive is restored on the router. 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 router.

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 router which is in factory default state, then during reboot, no backup is taken since no custom configuration file exists in the router by that time. The custom configuration is stored on the USB drive once the user clicks Save Settings in any GUI page.

Upgrading and Recovery Instructions:

Upgrading by using Web-UI

Please use GUI upgrade feature to upgrade to this firmware version. For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the *Unified Services Router v3.02 User Manual*

Recovery by using reset button

In case of device's firmware damage during firmware upgrade or uncertain issue, please manually access it by following steps: Power off the DSR-500AC/1000AC, press and hold the reset button, then power on and keep hold the reset button for over 15 seconds, the DSRC-500AC/1000AC will enter the Web Recovery Mode.

The IP address will be 192.168.0.1, and make sure to setup same IP segment for your PC/NB then access the Web Recovery Mode via browser.

SSL VPN Compatibility List:

SSL-VPN SPLIT TUNNEL & SSL-VPN FULL TUNNEL	
Windows 7 (32 bit)	IE-9.0, IE-11, Firefox 47.0.1
Windows 7 (64 bit)	IE-9.0
Windows 8 (32 bit)	IE-10.0, Firefox 47.0.1
Windows 8 (64 bit)	IE-10.0
Windows 8.1 (32 bit)	IE-11, Firefox 47.0.1.
Windows 8.1 (64 bit)	IE-11

New Features:

Firmware Version	New Features

3.10	1. PPTP/L2TP VPN Client auto dial-in feature
	2. Support User's group and group's privileges edit
	3. Updated max number of wireless clients
	4. Wireless IGMP Snooping support and Multicast to Unicast
	6. OSPF support on L2TP over IPsec
	7. Category filters for device logging
	8. Support configurable IPsec backup policy
	9. Support WCF 3-month trial license
	10. Support multiple OpenVPN clients with the same certificate
	11. Alerts via SMS for WAN/IPsec/CPU/RAM events
	12. Support source port configuration for custom services
	13. Multi-language support
	14. Support Omni SSLVPN client
	15. Select verified DDNS services:
	    a. DynDNS
	    b. D-Link DDNS
	    c. FreeDNS
	    d. NO-IP
	    e. 3322.org
	    f. Oray (existing in M7)
	    g. Custom

3.07	It's the first release.

Changes of MIB & D-View Module:

Problems Fixed:

Firmware Version	Problems Fixed
3.10	1. SQL injection Post authentication attack in Captive portal change password page. 2. WAN3 interface is unable in drop-down list of WAN interfaces on bandwidth profile page. 3. Unable to establish the SSL VPN tunnels in mac 10.6.8 host. 4. L2TP Over IPsec port option is not available in OSPF setting page. 5. Outbound firewall rule is not working for LAN to DMZ. 6. Unable to configure Static type and DHCP statefull on IPv6 WAN. 7. Unable to edit the subnet mask value in traffic selector page. 8. Unable to do default (factory default) from GUI. 9. Unable to detect the USB printer.

10. Unable to edit 2.4Ghz setting when WDS is enabled on 5Ghz radio

11. Able to establish WDS link even if the security modes are mismatched.

12. Still block URL even if blocked keyword is removed.

13. Unable to delete the users in specific case.

14. Unable to send logs to Gmail account from gmx sender mail address.

15. DSR PPTP Client doesn't stay connected with Windows PPTP server.

16. VPN Pass-through is unstable.

17. CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow.

18. Update SSL VPN certificate validity time.

19. Unable to Remote firmware upgrade through PPPoE WAN.

20. Support 64 characters for PPPoE password [DEUR20160217000004]

21. CVE-2015-3195: OpenSSL x509 _Attribute memory leak.

22. Unable to set WAN port speed. [DI20160310000002]

23. Configuration version is updated without a configuration change after reboot. [DI20160405000007]

24. Unable to establish OpenVPN client tunnel with Access server.

25. Unable to select multiple port in custom service of inbound bandwidth profile.

26. Unable to support IPsec main mode for iPad/iPhone Cisco IPsec client.

27. Dashboard information incorrect. DGC20160518000002

28. NTP service is not working for customized NTP server. [DGC20160614000003]

29. OpenVPN client mode is not work.

30. OpenVPN tunnel doesn't disconnect after OpenVPN server is disabled.

31. Unable to run traffic if PPPoE with DHCPv6 option is disabled.

32. Unable run traffic over PPTP client tunnel in MAC OS.

33. Passwords in configuration file is in plain text.

34. Unable to support NFS.

35. Unable to edit DHCP Reserved IP entry.

36. Reboot logs contains username and password of the WAN PPPoE credentials.

37. Add display active private routes in "IPv4 routes table".

38. Remove MAC traffic selector Match type option when the bandwidth profile is configured for Inbound traffic. [DEUR20160218000008], [DUSA20160726000001]

39. Ping packets are going out without NAT IP when WAN is configured with PPPoE in WAN auto-rollover.

40. User group login Policies should be also applied for SSH.

41. Unable to login SSL VPN Portal when internal and external user is configured with same name.

42. The critical page display on VPN>SSL VPN>SSL VPN Server Policy.

43. Incorrect session entries on Active session page.

44. WAN is coming up, when clicked 'RENEW' button in WAN status page even though routing mode is configured as Transparent.

45. Unable to support FQDN Sever address for L2TP in WAN setting. [DRU20160126000002]

46. Unable to configure hash key (-) in PSK field for IPsec policies.

47. DHCP relay is not working over VLAN.

48. Support 32 bit mask for private static routes with destination as single IP.

49. DHCPv6 server is not giving lease to the clients who sent IAID as zero in request packet.

50. Application rule is still working even if the rule is disabled or deleted.

51. Unable to add second routing **policy** with same service at protocol binding.[DGC20160520000003]

52. Unable to show connected network printer on Windows7.

53. Error display on Wi-Fi schedule control. [DGC20160614000003]

54. UPnP device is not showing correct name in the host

55. Unable to continually play Audio stream from specific server.

56. Support PPPoE MSS auto-detect. [DI20160509000004]

57. Deleting the conntrack entry of ICMP reply packet from WAN.

58. unable to ping 8.8.8.8 through L2TP/IPSec tunnel from Windows client.

59. 3G connectivity is not coming up after reboot.

60. Unable to add SNMP Access list for same IP with different community and privileges.[DI20160706000002]

61. Adding Help content in "Aprroved Urls" page for approved URls priority is wrong.[DUSA20161014000002]

62. Incorrect WAN link speed status in CLI [DI20160531000002]

63. Unable to configure PPTP client IP pool in LAN Subnet. [DRU20160623000003]

64. Unable to get IP using DWM-156 A3. [DEUR20160627000005], [DEUR20160822000002]

65. Showing wrong VLAN info.

66. DDNS status message is not displaying properly when there is symbol # in the password.

67. Unable to change 20Mhz to 80Mhz in 5Ghz radio setting. [DGC20160618000001]

68. Dashboard information incorrect. [DGC20160518000002]

69. Support 80Mhz channel spacing for Russia [DI20160615000002]

70. Support 48 characters for email address. [DUSA20160831000003]

71. CVE-2016-5696: "Off-path" TCP exploits.

72. Insecure RSA public keys in TLS certificates for GUI login and OpenVPN.

73. Unable to send logs to Gmail account from gmx sender mail address. [DEUR20151113000006]

74. CLI command to show port link speed is displaying port speed value even WAN link is down. [DI20160531000002]

75. Unable to configure PPTP client IP pool in LAN Subnet. [DRU20160623000003]

76. Able to configure WAN mode in load balancing even when user configured configurable port as DMZ.

77. Unable to support full tunnel for remote L2TP over IPsec client [DUSA20160723000002]

78. Configuration is getting increased with reboot even without a configuration change. [DI20160405000007]

79. 5G Channel display "frequency", not "channel" in wireless status page.

80. Showing wrong VLAN info in the WebUI. [DEUR20160421000005]

81. DDNS status message is not displaying properly when there is symbol # in the password. [DEUR20160421000005]

82. Sometimes device is getting crashed while changing radio settings frequently under wireless traffic. [DGC20160618000001]

83. Low throughput in NAT mode with PPPoE wan type. [DI20160509000004]

84. Dashboard information incorrect. [DGC20160518000002]

85. 3G is not coming up after reboot. [DEUR20160325000004]

86. Unable to add SNMP Access list with same IP, Subnet Mask and different community, privileges. [DI20160706000002]

87. Maximum log entries are not reaching up to 1500 lines in GUI Page. [DI20160913000004]

88. Help content in approved Urls page description for approved URls priority is wrong. [DUSA20161014000002]

89. Unable to support DWM-157 B1 [DEUR20160913000002]

Known Issues:

Firmware Version	Known Issues
3.10	1. Ping loss while downloading 2GB files over SSL-VPN tunnel. 2. IGMP snooping is not work. 3. Unable to support SSL-VPN Split tunnel in WIN8.1 (32/64bit) with IE11 browser. 4. Unable to establish SSL VPN tunnel in Google Chrome v42 with Java 8 update 31. 5. Unable to establish SSL-VPN tunnels in MAC OS [10.10.4] "OS X yosemite". 6. Unable to establish SSL VPN tunnel with Opera (v34) 7. Unable to connect wireless client from untagged interface in SSID trunk mode. 8. UPnP Port Map List entries are not getting flushed from device after the skype session is terminated. 9. Unable to accept "Authentication server1/2/3" fields with server name. 10. Unable to show internal IP address field while adding the inbound firewall rule over WAN2 when WAN1 is in classical routing mode. 11. Unable to access Intel AMT over port forwarding tunnel. 12. SMS alert functionality is not working when WAN mode is configured as auto rollover between WAN1 & WAN2. 13. Some traffic loss when IPsec client behind NAT device. 14. Unable to reach DUT LAN interface over IPSEC tunnel when WAN Mode is configured as load balancing. 15. SSL portal with Radius_pap authentication is not logged in with external radius_pap user when portal added through snmpset. 16. SNMP trap port incorrect and unable to receive SNMPv3 traps. 17. Unable to show WAN information on Dashboard in RU firmware. [DBG16120345] 18. Able to send WAN1 IP through WAN2 interface in Protocol-Binding. [DBG17010033] 19. Unable to limit the number of user and user group as specification. [DBG17010021] [DBG17010030] [DBG17010031]

Related Documentation:

- Unified Services Router User Manual v3.02
- Unified Services Router CLI Reference Guide v1.10