Firmware Version: 2.11_WW
2.11_RU
Published Date: Jan. 15, 2016

Copyright Notice

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:

Firmware Version	Region	Date	Model	HW Version
2.11_WW 2.11_RU	WW/RU	Jan, 15, 2016	DSR-150, DSR-150N, DSR-250, 250N	A2/B1
2.02_WW 2.02_RU	WW/RU	Mar, 05, 2015	250N	B1
2.01_WW 2.01_RU	WW/RU	Oct, 20, 2014	DSR-150, DSR-150N, DSR-250, 250N	A2
1.09B32_WW 1.09B32_RU	WW/RU	Mar, 14, 2014	DSR-250, 250N	A1/A2
1.08B44_WW 1.08B44_RU	WW/RU	Oct. 28, 2013	DSR-250, 250N	A1/A2
1.08B39_WW 1.08B39_RU	WW/RU	Oct. 23, 2013	DSR-250, 250N	A1/A2
1.08B31_WW 1.08B31_RU	WW/RU	Jun 28, 2013	DSR-250	A1/A2
1.05B53_WW 1.05B53_RU	WW/RU	Jun 29, 2012	DSR-250, DSR-250N	A1
1.05B20_WW 1.05B20_RU	WW/RU	Mar 28, 2012	DSR-250, DSR-250N	A1
1.05B20_WW 1.05B20_RU	WW/RU	Mar 28, 2012	DSR-250, DSR-250N	A1
1.05B20_WW 1.05B20_RU	WW/RU	Mar 28, 2012	DSR-250, DSR-250N	A1
1.01B56_WW	WW	Oct. 06, 2011	DSR-250N	A1
1.01B46_WW	WW	Sep 23, 2011	DSR-250N	A1

Important Notes:

1. Automatic factory reset when image upgrade detects a firmware region mismatch between RU and WW images. Such as firmware upgrade from RU->WW or WW->RU image.
2. The switching between RU & WW images will initiate an automatic factory reset. The feature differences between these images are significant and can only be aligned with a reset of the configuration.
3. Russian firmware version doesn't support over 56bit encrypted algorithm according to regulatory restriction.

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

5. 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)
6. 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. It will take around 3 minutes at least for this case.
7. DHCP reserved IP feature is changed to support "inside DHCP IP pool range" in order to meet common behavior in networking industry. Old DHCP reserved IP entries will still be valid. When creating a new DHCP reserved IP, it has to follow newer behavior.
8. Now we support following 3G dongles:
   D-Link: DWM-152 A1, DWM-156 A1/A3/A5/A6/A7, DWM-157 A1/B1, DWM-158 D1 and DWP-156 B1 and DWP-157 B1, HUAWEI: E1550, E173, EC306 and E303
9. Before plug DWM-152/156/157/158 3G USB dongle, please make sure the SIM Card is NOT set PIN code.
10. 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 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 v2.00 User Manual.*
- **Please upgrade corresponding firmware based your device hardware version.**

New Features:

Firmware Version	New Features
2.11	1. PPTP/L2TP VPN Client auto dial-in feature 2. User's group and group's privileges edit support 3. Updated max number of clients 4. Wireless IGMP Snooping support 5. LAN IGMP Snooping support (DSR-250/250N only) 6. OSPF support on L2TP over IPsec 7. Category filters for device logging 8. Support configurable 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 for DSR-250N B1 14. 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
2.02	1. CPU watchdog support, the device will reboot once CPU overload. PS : CPU watchdod is ebale by default, but it can be disable via CLI command « *util watchdog_disable Y* » 2. Update SSL VPN compatilbility support list for Window 8.1 and Browser version.
2.01	1. Brand new GUI design 2. Dynamic Web Content Filtering (Subscription is required). 3. Supporting DHCP ranges for all subnets. 4. VLAN on WAN for single VLAN ID. 5. Supporting web GUI access by a particular IP or VLAN. 6. SSLVPN authenication support external user DB.

1.09B32	1. L2TP client mode enhancements: support MPPE and demand dialing. 2. User DB enhancements: support PPTP/L2TP tunnels external authentication though AD, LDAP and POP3. 3. Support Selectable Outbound Interface for IGMP [HQ20121210000012] 4. Proxy ARP: Allowing PPTP server range in range of LAN 5. CLI enhancements: support the "space" character 6. Web GUI enhancements: support auto parameters fill-out in the DHCP server configuration page 7. 3G dongle supports: add Huawei E303, D-Link DWM-156 A7, D-Link DWM-157 B1, and D-Link DWM-158 D1. 8. A new click button to quickly download Dbglogs. 9. A new checkbox to enable/disable auto config backup. 10. A new checkbox to enable/disable config file encryption. 11. Support a Windows-based config viewer for encrypted config files. 12. Support L2TP VPN client mode. 13. Support 5 concurrent GRE tunnels. 14. Lengthen IPSec Pre-shared key length to 64 characters. 15. Simplify IGMP settings – allow all net to pass through DSR by default. 16. Add package manager with single selectable 3G driver support 17. Change IP address setting for inbound traffic management to configure LAN IP from server IP.
1.05B53	1. Support email address to be local ID in Ipsec policy. 2. Support SHA-1 in Phase 1. 3. Support DH group need support group 1, 2 and 5 for Phase 1. 4. Add PFS group 1, 2 and 5 for Phase 2. 5. Add a keyword with "." (dot) in Blocked Keywords text box.
1.05B20	1. Support 3G dongle DWM-152 A1/A2/A3, DWM-156 A1/A2/A3, Huawei E1550, E173. 2. Pre-Share key can be configurable in wireless wizard. 3. Change design to disable auto refresh for Traffic Monitor by default.
1.05B06	Support SSH remote management from WAN port
1.01B46	It's the first release.

Changes of MIB & D-View Module:

Firmware Version	New Features
1.05B06	Support LED and IPsec MIB.
1.01B46	It's the first release.

SSL VPN Compatibility List:

SSL-VPN SPLIT TUNNEL & SSL-VPN FULL TUNNEL	
Windows-XP	I.E-8.0, Firefox 16.0.1, Opera 12.0.2, Google Chrome 22.0.1229.96m
Windows-Vista	I.E-8.0, Firefox 33.1.1, Opera 26, Google Chrome 40.0.22.09
Windows 7 (32 bit)	I.E-9.0, I.E-10.0, Firefox 33.1.1, Opera 26, Google Chrome 40.0.22.09
Windows 7 (64 bit)	I.E-9.0, I.E-10.0
Windows 8 (32 bit)	I.E-10.0, Firefox33.1.1, Opera 26, Google Chrome 40.0.22.09
Windows 8 (64 bit)	I.E-10.0
Windows 8.1 (32 bit)	Firefox33.1.1, Opera 26, Google Chrome 40.0.22.09
Fedora 13	Firefox 33.1.1, Opera 12.0.2, Google Chrome 22.0.1229.96m
MAC-10.4.11	MAC Firefox 3.6.15, MAC Safari 4.1.3(45533.19.4)
MAC-10.6.8	MAC Safari 5.1.7.0, MAC Firefox 33.1.1

Problem Fixed:

Firmware Version	Problems Fixed
2.11	1. Unable to establish L2TP over IPsec tunnel if phase1 encryption is different from phase2's encryption. 2. When traffic is sent from WLAN to LAN or WLAN to WLAN, then data transmission rate is varying drastically. HQ20120820000010 3. There is an error logging when we enable WPS and click on push button. HQ20140205000021

	4. Supported Encryption fields in PPTP server page are not showing after applying on the save button. 5. Unable to install packages and device is showing message as "Not installed". 6. User is able to configure security mode in WEP or WPA+TKIP even though wireless radio mode is configured as NG or AN mode 7. Device is not accepting FQDN names in Server Address field when wan type is PPTP/L2TP 8. IPsec tunnel is not disconnected after changed policy from auto to manual. 9. Kernel panic in VPN-IPsec HUB & Spoke. HQ20140822000014 10. SSL VPN authenticated by external POP3 server fails. 11. Unable to get email logs in long duration test. HQ20141121000009 12. VLAN port members are not displaying in Port membership for VLAN under IGMP snooping page. 13. Device is not displaying pop-up message while changing the group's privileges. 14. Unable to access internet from wired or wireless LAN hosts after reboot when default AP is disable and custom AP is enable. HQ20150424000012 15. Error message is thrown when we edit or delete a user from the local database. HQ20150528000004 16. HTTP throughput is unstable in the remote setup. HQ20150529000018 17. Unable to change LAN subnet after changing device mode from NAT to Transparent 18. Port speed status is shown incorrectly when doing SNMP walk for LED MIB. HQ20150525000009 19. Unable to access web GUI from LAN host with Firefox v39. HQ20150717000006 20. Unable to download a file from a website in specific scenario. HQ20150601000006 21. IPSec tunnel is not getting established and there are no logs for the failure. 22. Unable to change LAN settings when device is in transparent mode. 23. Unable to connect L2TP over IPSEC tunnel on WEBUI. 24. Unable to configure more than 5 characters for community in snmp traps settings page.HQ20150827000008 25. Device should not throw any error while enabling Multicast to Unicast Setting in Advance Radio settings page irrespective of IGMP is enabled or not. 26. Configurable backup policy edit does not work. 27. IPsec tunnel VPNs Dashboard is not properly display the VPN status.

	HQ20150820000016 28. Multicast to Unicast conversion is not working properly for LAN to WLAN. 29. Enable 3DES encryption algorithm for phase 1 and phase 2 by default. 30. Unable to change the date and time after the WCF free trial expiration. 31. Multicast To unicast conversion is not working after editing the Wireless Profiles 32. Unable to receive SMS from DWM-158 D1 dongle. 33. Update certificate validity time for SSL VPN clients. HQ20151002000003 34. IPsec logs are not coming to syslog server when user try to establish secondary tunnel with different IKE version between same devices. 35. Remote management functionality is not working after reboot with all logs enabled in the device. 36. Device allows invalid configuration for traffic selector when the user adds custom service with multiple ports. 37. DUT showing prefix length field when source hosts or destination hosts option is selected with 'Single' in IPv6 firewall rules. 38. Critical error observed when we click on the 'Export Logs' button in All Logs page. 38. Remote firmware upgrade through PPPoE WAN is failing. HQ20151026000019 39. Wireless VLAN in general mode is not working for tagged interfaces. 40. No NAT translation of SIP headers during REGISTER, outbound call and SDP packet 41. Support IKEv2-SHA2-256/384/512 algorithms. 42. Inter-ISATAP subnet routing is not working. 43. After changing channel spacing 20/40 MHz to 20 MHz in UPPER band channel as auto, beacons frames are not updating accordingly. 44. Not able to enable WPS for custom profile with WPA/WPA2 security mode. 45. Able to edit and delete custom service associated with traffic selectors. 46. When "block ICMP" is configured for a SSL VPN policy with permit permissions, ICMP packets over SSL VPN tunnel are not getting blocked. 47. Transparent mode functionality is not working. 48. Not able to run TCP traffic over IPV6 IPsec GW-GW/manual tunnel with des/3des/blowfish/CAST128 as encryption algorithm 49. 3G support to be extended to Static Routing. 50. Unable to run FTP and HTTP traffic on PPPoE over IPv6 connection due to MTU size problem 51. Device not showing physical interface IP address in WAN status & router

	status, when it is connected to Russian dual access PPTP. 52. Unable to add static route on physical interface if wan is configured to Russian dual access PPPoE with physical interface is configured to dynamic. 53. Remove SSL VPN logs page in Russian firmware. 54. Unable to reach ipv6 wan host through ipv4 and ipv6 PPTP tunnel from PPTP client. 55. Able to establish IPsec VPN GW-GW tunnel, able to authenticate captive portal with 'Extended Authentication' NT-Domain when NT-Domain Wrong Work Group configured. 56. Unable to login to the counter strike game when device WAN is configured for L2TP. 57. Support GRE tunnel functionality for 3G. 58. Device is not showing correct status in current channel field of Radio settings page and WLAN status page when Default AP is in disabled state. 59. WPS LED is not working. 60. Dhcpv6 client process got killed after reboot/restore when wan type as PPPoE with stateless/stateful. 61. Unable to mount the files using NFS service. 62. DHCP relay process for VLAN is not running before WAN is up 63. Unable to re-connect the PPTP clients once they get disconnected. 64. Unable to upload the URL csv file in the device and GUI is getting stuck at this page. 65. IPsec tunnel is not getting auto establish after reboot. 66. Device is not accepting IP address with last octet 0 or 255 even if it is within the subnet. 67. Multiple VAP active is not getting enabled or disabled with device time after reboot. 68. Unable to access GUI when PPTP client is configured without remote_network and timeout. 69. Unable to open USB shared folders in RU firmware. 70. Unable to run traffic to the remote host over PPTP/L2TP clients, when default policy is blocked. 71. Allow RSA generated server key in OpenVPN certificate upload page 72. Mac book (connected as the wireless client) stop receiving the MDNS packets. 73. Blocked Keywords and Block All URL has lower priority than dynamic content filtering. 74. Disallow editing of IPsec policy if one to one NAT has been added on that

	policy. 75. Device not showing the PPTP /L2TP connected users in PPTP/L2TP Active users page when PPTP/L2TP client tunnels established with External Authentication. 76. When wireless client is connected through WPS, remaining clients which are already connected with WPA are getting disconnected. 77. Unable to run the traffic on PPPOE interface when VLAN on WAN is configured for Russian Dual Access PPPoE. 78. IPsec tunnel is not getting established when DUT is in behind NAT Topology. 79. Device is not showing the current channel field in Radio settings page. 80. VLAN host is not getting IP from custom VLAN if we enable DHCP server with DNS proxy is enabled while adding custom VLAN. 81. Unable to get IP when we connect the wireless client with WEP 64/128 bit by configuring the ASCII number of characters. 82. Clients associated with the edited SSIDs are not able to browse websites. 83. Able to run the traffic to remote LAN host after disabling the PPTP client in RU firmware. 84. Unable to run traffic to the remote LAN host without refreshing the Active PPTP VPN Connections page After establishing the PPTP client tunnel. 85. Unable to assign group to default SSLVPN portal when firmware upgrade from 1.09B32 to 2.01. 86. OpenVPN configuration page is accepting device's LAN subnet as server network. 87. Unable to ping between two windows wireless clients when security mode is configured as WPA/WPA2/WPA+WPA2. 88. DDNS not getting updated after reboot. 89. After Device got reboots LAN DHCP leased clients page is not getting updated properly. 90. VPN backup functionality is not working properly when we plug and unplug the wan 91. SSL fallback Vulnerability: (CVE-2014-3566) 92. Vulnerability: CVE-2014-3568 Build option no-ssl3 is incomplete 93. Observed critical error while uploading IPsec policy with traffic selector type as ANY 94. Attacker is able to reset legitimate TCP connections with the device leading to denial of service. 95. Inter VLAN firewall rules are not updated properly.

	96. Unable to establish SSL VPN tunnels using Firefox/opera/chrome in windows 8.1/8/7 (32 bit version). 97. WiFi channel is automatically goes to channel 1 if we select channel 12/13 for the country EU_Norway. 98. LAN Configuration page is accepting configured OpenVPN network as device's LAN subnet range. 99. Unable to get syslog via IPsec tunnel. 100. WDS functionality is not working 101. Observed critical error page in Maintenance --> Firmware and Upgrade->Update firmware->USB in Use page. 102. Unable to configure user to DNS host name and IP mappings when DHCP reserved IP entry is added. 103. Unable to access the WDS page after enabling WDS. 104. L2TP client is able to connect the device with Local database authentication when L2TP server is enabled for POP3 authentication. 105. Unable run traffic over PPTP client tunnel in MAC OS. 106. Unable to change LAN subnet after changing device mode from NAT to Transparent and Transparent to NAT. 107. IP/MAC binding, Block MAC and Firewall rule are higher priority than category filtering. 108. Bridge firewall rule functionality is not working when firewall rule is configured with custom service type "both". 109. Able to configure WEP/WPA(TKIP) security mode when radio settings is configured in mixed N or N only mode. 110. After changing the encryption type in IPsec policy(Protocol:AH) ,it was not reflected in the Device 111. Unable to do SSH to device from LAN side. 112. Fix for OpenSSL Vulnerabilities 2014-3569, 2014-8275. 113. L2TP server and L2TP client logs are not coming in L2TP-Client or L2TP-Server category. 114. Wireless client not able to ping remote LAN host over IPsec tunnel. 115. WCF related logs are not coming. 116. Spoke to Spoke traffic is not going through IPsec Tunnel in Hub-Spoke Set-up 117. USB/printer sharing configuration should not be disabled when USB/printer is disconnected. 118. Error in configuration of VLAN with subnet 255.255.255.252. 119. The device is showing "Checksum failed" message while uploading the

	configuration file. 120. IGMP snooping functionality is not working after factory default the device. 121. Not able to delete the user which group's user type is configured as network. 122. Response of NAT Loopback for RTP is not working properly. 123. Apply changes for vulnerability CVE-2015-0291 / CVE-2015-0204. 124. Support source port in custom services. 125. Unable to run http traffic over ipv6 network when device wan is configure with ipv6 PPPoE. 126. Device is losing prefix delegation information after reboot. 127. Unable to configure DUT as IPsec policy with L2TP mode as client and direction type as responder. 128. Device showing the IPsec mode as tunnel mode in IPsec policies list even though we configure the IPsec mode as transport mode. 129. NAT functionality not working when switched back to primary WAN in Auto-Rollover mode. 130. Loosing GUI access when VPN remote network is configured in lan subnet. 131. Observed kernel panic while working with PPPoE connection type with DynDNS configured in DUT. 132. IPsec Keep alive functionality is not working. 133. Classical routing mode functionality is not working.
2.02	1. Can't set WIFI channel 13. HQ20141114000016 2. Can't support bandwidth management by Port Name for inbound traffic. HQ20141114000016 3. Unable to ping between two windows wireless clients when security mode is configured as WPA/WPA2/WPA+WPA2. HQ20140828000012 4. DSCP packet TOS value showing default value instead of configured in some of the packets at HUB. HQ20140619000012 5. Schedule setting can't be applied into the same service in firewall rule HQ20140522000005 6. Issue with Port forwarding (HTTPS/PPTP) HQ20140701000006
2.01	1. In SIP ALG disable state, User is able to establish multiple calls from WAN->LAN and LAN->WAN 2. IGMP proxy daemon is not running in the back-end with IGMP proxy enabled when WAN mode is in load-balancing

	3. Attacker is able to reset legitimate TCP connections with the device leading to denial of service. 4. **Security Vulnerabilities Addressed**: TCP/IP Sequence Prediction Blind Reset Spoofing DoS. CVE: CVE-2004-0230 5. Inbound http service (HFS http file server) is not working in ADSL PPPoE ISP 6. Unable to access internet or low throughput performance for WLAN clients while one of WLAN client is running HD video streaming. 7. PPTP pass-through priority is highest than PPTP firewall service. 8. IPSEC pass-through priority is highest than IKE outbound firewall service. 9. WLAN PC can't play multicast stream 10. USB storage not working perfectly with windows XP. 11. SIP module is inserted failure after reboot 12. The Login Profiles in SSL VPN are not persisting after device firmware upgrade and Reboot. 13. When WAN Mode is configured for WAN1 dedicated, but WAN2's IP alias is able to run traffic for inbound rule added. 14. "loggingd" process got killed in QA-Gateway with attached configuration. 15. IPSEC tunnel can't established after importing the exported file at the remote device until disable then enabling policy 16. Device is not updating time after every GUI change in "Timezone" page. 17 User can't establish IPV6 ipsec gw-gw/manual tunnel using both local & remote 18. Active vpn status is not displaying proper information when vpn policy is added with mode config in the device and DHCP over ipsec in client. 19. Observed lua error upon upgrading the device with customer configuration to 1.07B58_RU image using IE8 browser. 20. Http access from wireless clients to wan is taking long time from wireless client 21. Device showing "Authentication Failure" message only once for wrong credentials. 22. Device is accepting the SMTP mails when Default Outbound Policy configured as "Block Always" without configuring the SMTP Rules (Approved Mail, Blocked Mail, and Subject List). 23. Device is not releasing IP configuration for WAN1 fail over to WAN2 when other device acting as DNS provider 24. Wireless clients can't ping after editing the wireless Access-point from one profile to another until disable then enable wireless AP again. 25. OpenVPN static IP doesn't work in 1.09B32

	26. Remove auto dial support from both PPTP and L2TP Client pages HQ20140801000005 27. Unable to see the External WAN IP in the HTTP server for the in-coming traffic from WAN but showing source IP as DMZ IP address HQ20140717000007 28. Unable to configure the subnet mask 255.255.255.128 from CLI while configuring traffic selector rule. HQ20140804000003 29. Support maximum external 2TB HD HQ20140110000009 30. Unable to ping between two windows wireless clients when security mode is configured as WPA/WPA2/WPA+WPA2 HQ20140828000012 31. **Security Vulnerabilities Addressed**: OpenSSL 0.9.8x does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability. 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: Patched OpenSSL to 0.9.8za
1.09B32	1. L2tp internet connection problem HQ20120810000001 2. Device wan is unable to come up with 3G ISP with DWM-156 A5 dongle. 3. Unable to pass Netperf traffic over IPsec tunnel. 4. The throughput of WAN Routing mode is much lower than the WAN NAT mode. 5. Traffic should run over the VPN client tunnel even when SPPE is in enabled state. 6. Support NCP vpn client is able to access VLAN subnet. HQ20120827000010 7. Support ARP from WAN HQ20120926000011. 8. Update all pages copyright notice to 2013. 9. Disabled firewall rule can't be deleted. HQ20130126000001 10. SSL VPN xtunnel.cab Certificate page valid date is from 8/13/2010 to 8/13/2012. HQ20130205000011 11. After initiating traffic from WLAN->LAN wireless client is getting disconnected and unable to reconnect.

	12. Manual time change event is not getting logged 13. Kernel panic while running traffic from WLAN/LAN hosts to internet and running traffic over IPsec tunnel when device wan is configured with L2Tp ISP. HQ20130325000004 14. when device wan is configured in l2tp+dhcp mode, device is sending ddns membership packets to dns ip assigned by dhcp server HQ20130325000004 15. Able to login to the portal with when configured wrong secret in the radius settings page 16. Unable to get the IP for PPTP client in the device. 17. Device can't detect the printer 18. Http and FTP traffic can't be transferred over IPSEC client tunnel. 19. Transparent mode functionality is not working. 20. Device time will not synchronize with default NTP servers after reboot. HQ20130425000006 21. Not able to establish L2TP over IPsec tunnel with same user multiple time after making changes in IPsec policy. 22. Unable to find getuserDB page in RU images. HQ20130807000009 23. Unable to edit Roll-over WAN(3G) setup page. 24. Changed configuration in the configuration file is not persisting after restoring the configuration file into the device 25. User is unable to restore the encrypted configuration file into the device 26. Encrypted configuration file is not getting decrypted if we open the encrypted file from configtool. 27. Configuration is not getting saved into the USB, After enabling the 'Enable Autobackup' field. 28. No option to configure VLAN port membership for Port5, Port6, Port7 and Port8 through CLI. 29. Unable to get IP address to VLAN host after reboot. 30. Device is not showing any warning when trying to add duplicate VLAN ID. 31. DMZ configuration page is not available in GUI. 32. User not able to configure DNS proxy in LAN configuration page, even after PPTP server disabled 33. Bandwidth Profile Rate Functionality is not working.

	34. Kernel panic when trying to connect L2TP client over IPsec. 35. SSID can't broadcast when wireless is in open mode and radio setting is n client. 36. MAC address field is showing empty in WDS page. 37. Add Help content for DMZ pages 38. DMZ related fields are not getting highlighted immediately after enabling the DMZ option. 39. Error message should be proper when user tries to check updates in manager page without internet connection. 40. Unable to enable DMZ from CLI. 41. Unable to add IPsec gw-gw policy and firewall inbound rule on rollover WAN (3G WAN). 42. Unable to establish VPN connection in phase2 with SHA-256. HQ20130204000013 43. Low InterVLAN download speed. HQ20130620000004 44. VLAN, PPTP Server, L2TP server, and SSL client ranges and DMZ in same subnet. 45. Unable to take Packet Capture on DMZ interface. 46. Port translating field doesn't update in CLI after firewall rules is changed in GUI. 47. Unable to upload .CSV file. 48. Device is displaying WLAN edit configuration page for VLAN through CLI. 49. Synchronization Select Interface options of UPNP in CLI and GUI. 50. Showing wrong firmware version in SSLVPN portal page. 51. Able to configure the DMZ configuration without enabling the DMZ. 52. User is not able to access the device CLI using SSH. 53. Device is getting default when downgraded from 1.09b08.img to 1.08b39.img. 54. No options are available for VLAN configuration on wan page from CLI. 55. Unable to upgrade the firmware via USB. 56. Error message should be proper when we try to add DMZ reserved entry without DMZ enabled.

	57. LAN host can't receive 6 to 4 prefix radvd IP from the device. 58. Device is showing '***failed to open ?directory' in CLI when log in by telnet. 59. Kernel panic while running traffic over VPN tunnel. 60. IPS signatures can't be loaded if IPS is enabled. 61. ISATAP functionality is not working. 62. PPTP client status through CLI is showing "Disconnected" even it is connected. 63. Interfaces are not displaying when user configures status route through CLI. 64. Improve PPTP performance. 65. Improve RFC 2544 UDP performance via IXIA. 66. Support DHCP option 66 67. Unable to establish the IPv6 IPSec tunnel after edit the policy. 68. GW-GW tunnel can't be established when traffic selectors "Subnet--Range". 69. Outbound traffic over IPsec tunnel is blocked when default outbound policy is configured "block always". 70. No option for L2TP mode in CLI when IPsec policy is added. 71. Kernel panic while executing VPN manual tunnel automation scripts. 72. Device is showing entry for the wireless clients which are trying to authenticate in "wireless clients page". 73. Need to regenerate self--signed certificates. 74. Unable to establish GRE tunnel when WAN ISP type is configured for PPTP/L2TP. 75. DNS request timeout in LAN host by nslookup when IPS/IDS is enabled in the device. 76. Unable to connect PPTP server using LDAP External Authentication. 77. Unable to connect L2TP server using LDAP External Authentication. 78. "configuration could not be saved" message when user done any configuration through CLI for the first time. 79. Getting critical error when clicked save button in DHCP Reserved IP address page after upgrading from 1.01B46. HQ20130827000010

	80. Need username and password fields for open VPN client authentication in open VPN configure page. HQ20130724000015 81. Custom VAP active can't be enabled or disabled for device time. HQ20130917000005 82. SSID "DSR-250N_2" can be visible if the user configure "active time" but disabled the VAP. HQ20130902000003 83. VLAN firewall rule is not work. HQ20130930000008 84. Default SSIP can be visible even though WIFI disable. HQ20131108000016 85. Need to remove the Debug log after device gets bootup in serial console. HQ20131217000002 86. Change source IP address option for inbound traffic selector to destination IP address. HQ20140121000011 87. LAN client page is not displaying the connected LAN clients. 88. When the GRE tunnel is established, local PC ping to peer DSR's LAN IP address can't get response. 89. Usage of extended authentication when redundant gateway check---box is enabled.
1.08B44	**1. 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) **Solution:** Remove all unnecessary root user accounts 2. After rebooting devices, synchronization with NTP didn't works. (DRU20130424000003) 3. Firewall rule with scheduling is not work. (DUSA20130125000001)
1.08B39	1. Including 1.08B31 all fixes for DSR-250N in this version 2. The MPPE function does not work in L2TP client mode 3. Restore configuration file to different HW version 4. WAN responses ARP packet 5. Add a message to inform user, who need to change 443 port number for sslvpn or remote management once two features are enabled. 6. Can't work with any AP connected with network cable 7. Device time not synchronizing with default NTP servers after reboot. 8. Firewall rule disable is not work unless reboot device. 9. WIFI stability issue under heavy BT traffic

1.08B31	1. The OpenVPN Local Network page disappear when I used IE8 or IE9 to manage the DSR. 2. USB sharing could not download/upload large file 3. DWM-156 A3, A6 compatility issue 4. **Security Vulnerabilities Addressed:** Persistent root access. **Reference:** http://packetstormsecurity.com/files/118355/D-Link-DSR-250N-Backdoor.html **Solution:** Removed CLI commands that could allow someone to overwrite the super user password and gain root access to the device. Root user account will be completely removed in the next firmware version. 5. Prevent to upload config file into different model 6. Unable to change the Wireless output power 7. Device stuck under BT download 8. X.509 certificate expired issue 9. **Security Vulnerabilities Addressed:** uPnP vulnerabilities identified in the audit of libupnp code base. **Reference:** CVE-2012-5958, CVE-2012-5959, CVE-2012-5961, CVE-2012-5962, CVE-2012-5963, CVE-2012-5964, CVE-2012-5965 **Solution:** Patched Intel SDK libupnp v1.3.1 to add the following; 1) use 'snprintf' and 'strncpy' instead of 'sprintf' and 'strcpy', 2) While doing a 'strncpy', check if we are copying more bytes than the destination string size. 10. DNS query issue for L2TP WAN type
1.05B53	1. DSR-250 and 250N don't show Logs for tunnel disconnect and Logout for SSL VPN & port forwarding. 2. "LAN clients" page is not displaying the connected information. 3. CLI wan1 status does not show wan1 physical interface information when device is in RU firmware dual PPPoE mode. 4. When server IP is configured with FQDN, Wan L2TP over DHCP connection does not reconnect after device reboot. 5. Default VLAN is associated with all the wireless SSID after reboot. 6. "Block ICMP" is not work for a SSL VPN policy with permit permissions. 7. Traffic is not going from PPTP/L2TP client to device's LAN after changing

	WAN ISP until disable and enable PPTP server again. 8. When the user login SSL portal with wrong credentials domain name in IE browser address bar, the browser will not refresh back to 'SSL portal login' page. 9. Dyndns name provided in the SSL portal page will be changed into the device WAN IP, if the user try to login SSL portal page with wrong credentials in Firefox browsers. 10. Device's MAC address field in WDS page is blank in RU image. 11. Device is taking 40-50 seconds to apply the configuration in VLAN page of RU image. 12. Wireless client status page is showing wrong Authentication and Encryption types. 13. Device GUI is getting stuck after running bulk traffic over PPTP/L2TP tunnel. 14. "Connect" button is not working for IPv6 gw-gw policy in Active VPNs page when IPv6 WAN is radvd IP. 15. No information on WLAN Domain when country code is set to Japan. 16. Firewall rule with schedule is working correctly only for GMT time zone. 17. Device displaying critical error message when trying to upload certificates to activate OpenVPN server/client. 18. Unable to access GUI after factory reset and power OFF/ON the device. 19. Wireless clients are not getting updated in Wireless Clients status page. 20. UPnP process is not running in Dual Stack IPv4/IPV6 mode.
1.05B20	1. IPv6 to IPv4 tunneling is not work. 2. Internet web surfing is very slow for WLAN client if SPPE enabled. 3. Remove CLI command which is not supported in DSR-250/250N. 4. PPTP client is getting disconnected while uploading and downloading files using windows sharing. 5. Device shell is getting stuck after running bulk traffic over PPTP/L2TP tunnel. 6. Bandwidth Usage and Used applications are not displayed in dashboard. 7. Default VLAN will be associated with all the wireless AP after reboot. 8. Fixing L2TP doesn’t reconnects to L2TP server after reboot. 9. Fixing wireless clients is not displayed on status page.
1.05B06	1. Improving link up time of WAN interface less than 1 minute after device power on.

	2. Fixing the printer shared port detection issue. 3. Fixing PPTP pass through is not working. 4. Fixing SSL tunnel is disconnected when user tries to download 200 MB file.
1.01B56	1. Improving link up time of WAN interface to 1~1.5 minutes after device power on 2. Fixing PPPoE isn't working in custom MAC address

Known Issues:

Firmware Version	Known Issues
2.11	**<New Add>** 1. Device should not allow the user to configure remote management port with Reserved and Open ports which are already open in system. 2. SSL VPN and Port forwarding tunnel establish logs are not proper. 3. Static Routes and Default route are exchanging with metric 20 irrespective of the cost of interface for ospfv2.
2.02	**<Removed>** 1. Schedule setting can't be applied into the same service in firewall rule HQ20140522000005
2.01	**<New Added>** 1. No support for USB scanner 2. SNMP system alarm traps are not supported 3. voice at LAN side client is not heard when the SIP Proxy resides in LAN 4. Enhancement: Add sorting, filtering, searching operations to View logs page. 5. Daylight saving with manual settings is not working properly for Newfoundland and Greenland timezones. 6. After firmware upgrade, the OpenSSL tunnel is not able to established, the solution is to change a new OpenSSL port number in device UI, then change back to original port number again. (if the user don't want to change OpenVPN config file for the clients.) 7. Schedule setting can't be applied into the same service in firewall rule HQ20140522000005 8. Block Client is not work for Http service 9. L2TP, PPTP and IPsec pass-through is not work.

	<Removed> 1. PPTP pass-through is the highest priority than PPTP firewall service. 2. IPsec pass-through is the highest priority than IKE out-bound firewall service.
1.09B32	1. PPTP pass-through is the highest priority than PPTP firewall service. 2. IPsec pass-through is the highest priority than IKE out-boundf irewall service. 3. User is unable to add DHCP reserved for wired/wireless VLAN. 4. With 'Dlink DWA-160 Xtream N Dual Band USB adapter' the WPS status displays 'Failed' in the device WPS page, even though client is connected successfully. 5. Bandwidth rules over IPsec VPN tunnel are not being followed. HQ20120112000014 6. UPnp process is not running when wan link is down. 7. User is unable to print the file from wan host with inbound firewall rule. 8. Streaming/movie play is not perfect, when we try listen from LAN and VLAN hosts simultaneously. 9. Wireless VLAN in general mode is not working for tagged interfaces 10. Device should allow the user to configure UPNP on multiple VLAN subnets. 11. SIP ALG disable state User able to establish multiple calls from WAN->LAN and LAN->WAN. 12. Device nating the packet with WAN IP in Transparent mode. 13. Unable to drop tunnel by clicking 'Drop' button in active VPNs page after IPSEC VPN roll-over. 14. No option for SHA2-224 algorithm as 'Integrity Algorithm' while configuring IPSec phase-2 policy through CLI. 15. WPS Session status is not displaying the current status 16. Maximum static routes are not appearing in IPv4 Routing table and shell. 17. Unable to see logs when ips/ids are enabled. 18. Active VPN's page is displaying "IPsec SA established " even after clicking drop button when the device in behind NAT. 19. Client is not disconnecting after user time out exceeds in PPTP/L2TP server. 20. Device is not able to establish OpenVpn tunnel using IPalias.

	21. VLAN host can't get IPV6 address. 22. Client tunnel is not establishing with remote as single/range/subnet. 23. User is unable to establish IPV6 ipsec gwgw/ manual tunnel using both local & remote traffic selectors as any. 24. Upload speed for http traffic is fluctuating in the 500-1200 KBps over SSLVPN tunnel. HQ20120628000015 25. When traffic is sent from WLAN to LAN or WLAN to WLAN, then data trasnfer rate is varying drastically. HQ20120820000010 26. CLI can't support for L2TP client configuration. 27. Device is accepting the SMTP mails when Default Outbound Policy configured as "Block Always" without configuring the SMTP Rules (Approved Mail, Blocked Mail, Subject List). 28. VPN Tunnel is not re-establishing if we initiate traffic from client. 29. No GRE Tunnels status page in GUI. 30. Traffic selector rule for inbound bandwidth profile with match type as MAC address is not working. 31. Unable to add bandwidth profiles from CLI. 32. Unable to establish L2TP client tunnel when ISP is connected as L2TP. 33. Unable to establish L2TP tunnel with android phone when secret key is configured. 34. Idle time-out functionality is not working for PPTP users. 35. Multicast packets is sent to other LAN hosts when multicast traffic running from one LAN host 36. Specific Service support for inbound traffic management is not work.
1.08B39	1. PowerMode is not completely functional. 2. Wan is not getting IP from IPv6 DHCP server in stateful mode. 3. Netperf is unable to pass traffic over IPsec tunnel. 4. PPPoE performance worst if user changes the WAN MAC address.
1.08B31	1. PowerMode is not completely functional. 2. Wan is not getting IP from IPv6 DHCP server in stateful mode. 3. Netperf is unable to pass traffic over IPsec tunnel. 4. PPPoE performance worst if user changes the WAN MAC address.

	5. Device got defaulted after upgrade from 1.05B73_WW to 1.08B31_WW 6. Not able to establish L2TP over IPsec tunnel with same user multiple time after change IPsec policy. 7. The GRE function does not work 8. The MPPE function does not work in L2TP client mode.
1.05B53	1. Bandwidth Limit not functioning when port name is used in Traffic selector 2. PowerMode is not completely functional. 3. Wan is not getting IP from IPv6 DHCP server in stateful mode. 4. Netperf is unable to pass traffic over IPsec tunnel. 5. Transparent Mode is not supported. 6. Observed ping loss from WLAN clients to internet.
1.05B20	1. Bandwidth Limit not functioning when port name is used in Traffic selector 2. PowerMode is not completely functional. 3. Wan is not getting IP from IPv6 DHCP server in stateful mode. 4. Netperf is unable to pass traffic over IPsec tunnel. 5. Transparent Mode is not supported. 6. Traffic is not going to device's LAN from PPTP/L2TP client after changing WAN ISP, unless PPTP server disables and then enables again. 7. Observed ping loss from WLAN clients to internet. 8. USB file sharing transmission will be disconnected if file size is over 600MB.
1.05B06	1. Bandwidth Limit not functioning when port name is used in Traffic selector 2. PowerMode is not completely functional. 3. Wan is not getting IP from IPv6 DHCP server in stateful mode. 4. Netperf is unable to pass traffic over IPsec tunnel. 5. Transparent Mode is not supported.
1.01B56	1. WAN interface need to take 1~1.5 minutes for link up after device power on. 2. Bandwidth Limit not functioning when port name is used in Traffic selector 3. SSL tunnel is being disconnected when user tries to download 200 MB file

	4. Admin user is not able to SSH to device 5. Device is not detecting the printer shared port 6. Wan is not getting IP from IPv6 DHCP server in stateful mode. 7. Host MAC clone is not work. 8. Transparent Mode is not supported.
1.01B46	1. WAN interface need to take 2~3 minutes for link up after device power on. 2. Bandwidth Limit not functioning when port name is used in Traffic selector 3. SSL tunnel is being disconnected when user tries to download 200 MB file 4. Admin user not able to SSH to device 5. Device is not detecting the printer shared port 6. Wan is not getting IP from IPv6 DHCP server in stateful mode. 7. Host MAC clone is not work. 8. PPPoE isn't working in custom MAC address 9. Transparent Mode is not supported.

Related Documentation:

- Unified Services Router User Manual v2.00
- Unified Services Router CLI Reference Guide v2.00