Firmware Version: 3.19_WW/RU

Published Date: Aug. 19, 2021

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
3.19	WW/RU	Aug. 19, 2021	DSR-500AC/1000AC	Ax
3.17	WW/RU	May. 19, 2020	DSR-500/1000, DSR-500AC/1000AC	Bx, Ax
3.14	WW/RU	May. 02, 2019	DSR-500/1000, DSR-500AC/1000AC	Bx, Ax
3.13	WW/RU	Dec. 05, 2018	DSR-500/1000, DSR-500AC/1000AC	Bx, Ax
3.12	WW/RU	Mar. 26, 2018	DSR-500/1000, DSR-500AC/1000AC	Bx, Ax
3.11	WW/RU	Jul. 25, 2017	DSR-500/1000, DSR-500AC/1000AC	B1, A1
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. 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/A8, DWM-157 A1/B1/C1/D1, DWM-158 D1/E1 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 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 v3.13 User Manual*

DSR-500/500AC/1000/1000AC firmware support universal firmware for the different hardware version from v3.12. There are two firmware upgrade steps for firmware version v3.12.

Please upgrade firmware from v3.12B101.

If your device's firmware is earlier than 3.12, please upgrade corresponding firmware based your device hardware version.

Please follow the upgrade procedure in case fault caused during firmware upgrade.

1. Please check HW version on device UI first.
2. Select the corresponding intermediate and common firmware version for upgrade process.

Intermediate firmware
DSR-500_B1_FW3.11B001E_WW/RU
DSR-500AC_A1_FW3.11B001E_WW/RU
DSR-1000_B1_FW3.11B001E_WW/RU
DSR-1000AC_A1_FW3.11B001E_WW/RU
Common firmware
DSR-500_Bx_FW3.12B101H_WW/RU
DSR-500AC_Ax_FW3.12B101H_WW/RU
DSR-1000_Bx_FW3.12B101H_WW/RU
DSR-1000AC_Ax_FW3.12B101H_WW/RU

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 192.168.10.1, 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
3.19	1. Change default WIFI country code to DL domain, user can select WIFI country code after factory reset
3.17	1. Support VRRP 2. Force user to change default password. 3. OPEN SSL's client login URL is changed to https:/WAN IP/omnissl/
3.14	1. VLAN 1 support trunk mode 2. L2TP/PPTP support full tunnel 3. OSPF NSSA support
3.13	1. DNA app support. 2. OpenVPN supports manually establish tunnel. 3. WIFI transmit power setting is changed to % instead of dbm. 4. The number of firewall policy is shared for inbond and outbound. 5. OmniSSL support Win10. 6. OmniSSL support portal layout setting 7. Application Control (licensed by 3’rd party) 8. DUA-2000 External Captive Portal support. 9. SHA2 Hash Algoruthm support for generating OmniSSL certificate
3.12B101H	1. Improviding device throughput when Traffic managerment enable. 2. Bandwidth managemnt support by session number. 3. URL filtering support wildcard. 4. WCF support https protocol. 5. Improving logging content information. 6. WAN interface supoort Jumbo frame. 7. CLI support IPv6 and OpenVPN self cert. 8. OpenVPN support various authenication by userbase, Certicatate and TLS conbination.
3.11	1. Static route can be displayed in Route Information 2. Support HT80 for RU wireless Domain. 3. OmniSSL VPN support SSL Certification generation 4. IPv6 VLAN support. 6. Support VLAN/IPSec base Radius Authentication. 7. Hostname display support for DHCP clients. 8. Support RADIUS accounting and interim update. 9. Support IPv6 stateful and prefix delegation.

	10. Device support 3G/4G dongle with pin code password. 11. DWM-221 & 222 LTE Dongle support. 12. DWM-156 A8, DWM-157 C1 and DWM-158 E1 dongle support. 13. Support PPTP/L2TP client mode auto re-connect. 14. Support single IP or IP range to be Whitelist and Blacklist for URL filtering and Web Content Filtering.
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.

Problems Fixed:

Firmware Version	Problems Fixed
3.17	1. Sip client not able to registered with SIP server over ipsec tunnel if we initiated the SIP traffic continuously before establish the IPsec tunnel. HQ20191220000014 2. L2TP/IPSec VPN is ubale to use Active Directory authentication HQ20200317000007 3. IPsec tunnel may not establish if WAN failover is using DDNS HQ20191220000014 4. FreeDNS password is not support comma(,) and colon(:) HQ20200818000013 5. Open VPN Server and Open VPN Client Cant communicate between LANs HQ20200818000013 6. L2TP and L2TP/Ipsec tunnel is not establishing When the user configured WAN as Dummy ip and Ad server credentials as dummy and later we changed to correct one. HQ20200929000005 7. Character limit on server CN for new self signed certificates HQ20200827000001 8. Support more wildcard characters for authentication HQ20200911000006 9. The tunnel is unstable when IPsec policy is configured with FQDN HQ20200302000008 10. Not able to Activate WCF License when Existing License is Expired in Device HQ20201023000003 11. Openvpn maximum remote networks should be in sync with number of openvpn gw-gw tunnels HQ20201116000011 12. Device take over 10 mins to reboot by the particluar configuration HQ20201126000006 13. LED status for radio mode is not showing properly when custom access point involved HQ20201105000004 14. Able to configure broadcast IP address in the local server IP address of the inbound firewall rule HQ20210106000003 15. DAP cannot get IPv6 address from DSR HQ20210311000006 16. Device UI wil show critical error by particular firewall rules HQ20210423000007
3.17	1. Wan port speed graph on dashboard page is not showing properly. HQ20190319000009 2. "Device is in high performance mode" message is not showing on

	dashboard page if 'Traffic overview' button is disabled in Manage dashboard page. HQ20190514000007 3. User is able to add single address/address range as default Vlan IP address when selected as custom Vlan. HQ20190530000010 4. (>cpSockMsgHandler:763 failed to handle.) logs is displayed although Captive portal is disabled in the device. HQ20190605000005 5. Unable to send the email logs. HQ20190606000007 6. Device is showing error popup in OPENVPN page when user try to upload/generate certificates with backslash character. HQ20190621000018 7. IPsec tunnel cannot be established after factory and restore configuration. HQ20190611000014 8. L2TP tunnel is getting disconnected after 10 minutes even though "Reconnect mode - Always on" and "Auto connect" options are enabled. HQ20190730000008 9. License activation failed. HQ20190827000004 10. Time settings are loading incorrectly. HQ20190926000008 11. Lock the "Remote IP" to "Any" only if remote endpoint is FQDN. HQ20191016000008 12. Add logging for OpenVPN client connect and disconnect. HQ20200204000009
3.14	1. [CLI]system status WAN MAC address field is showing incorrect information, when WAN is configured as PPTP/L2TP/PPPoE HQ20190221000005 2. Getting critical error when we try to access openVPN related pages from page search. [RU firmware]DBG18110349 3. WAN3 statistics are not getting updated on the Dashboard page HQ20180910000003 4. Able to restore DSR-1000/A1 configuration into DSR-1000/B1 without any error but after device bootup unable to access or ping to the device. HQ20181018000014 5. OpenVPN related fields, OpenVPN related help content should be removed from application control pages. [RU firmware] DBG18110350 6. Device should not allow LAN IP address same as PPTP client address. DBG18110391 7. Device will reboot when the subnet mask of remote network is configured 32 in PPTP client page. HQ20190222000010 8. Turn off the debugging log for device logging. HQ20190221000004 9. Device should show proper error message when user try to upload RU

	image in Non-Russian version machine. DBG18110234 10. Need to DROP invalid state TCP packets received. HQ20181115000020
3.13	1. Remove BSSID from traffic selector 2. OmniSSL tunnel keep disconnecting after 20sec HQ20171127000003 3. Unable to add out of LAN subnet for firewall rule HQ20170731000017 4. Unable to save VLAN settings when PPTP/L2TP server's client IP address range is configured VLAN subnet HQ20180430000005 5. WCF for Https is not blocked properly HQ20180416000010 6. No openvpn logging entry HQ20180419000014 7. Unable to configure x.x.x.0 IP address in GRE setting HQ20180601000011 8. Weakness in user data validation (reflected cross-site scripting) (CVE-2018-6212) HQ20180531000002 9. Able to set the SSID with spaces from CLI, but not able to configure the same from GUI HQ20180606000002 10. Traffic selector setup page error HQ20180704000009 11. The number of L2TP tunnel can't reach specification HQ20180705000012 12. Max bandwidth is limited 100Mbps for bandwidth management HQ20171204000003
3.12B101H	1. L2TP over IPsec disconnect after reboot or logging enable. HQ20170120000005 2. Failed restore config due to large file size. HQ20170309000002 3. WAN auto-Rollover is not work. HQ20170612000008 4. Logging ascending issue. HQ20170911000008 5. OpenVPN and OmniSSL can't access the configured network. HQ20171016000004 6. L2TP over IPsec VPN with AD or NT Domain authentication is not work. HQ20170515000012 7. Unable to click "Details" button on Dashboard for Traffic Overview tab. HQ20170413000009 8. CVE-2017-14491 Dnsmasq Vulnerability. 9. SMS alert functionality is not working when WAN mode is configured as auto rollover between WAN1 & WAN2. 10. Unable to connect wireless clients on untagged interface when SSID is configured with trunk mode. 11. SMS functionality is not working until changing WAN mode from WAN1 to WAN3 with DWM-156-A7 dongle. 12. IPsec clients connected behind NAT will have traffic loss

	13. Unable to reach DUT LAN IP over IPSEC tunnel when WAN Mode is configured as load balancing. 14. User based OmniSSL server policy is not working if custom OpenVPN network is configured in OpenVPN settings page. 15. Unable to configure more than 16 characters for username and password of PPPoE WAN Type. HQ20170103000005 16. Unable to access GUI after change default VLAN IP network. HQ20170207000017 17. WAN is probably link down if the cable is plugged during device boot up. HQ20170413000006 18. Static DNS IP is required when static IP is configured for WAN interface. HQ20161213000003 19. Unable to generate the OPENVPN certificate when user input the space characters while creating OPENVPN certificates. HQ20170628000012 20. Unable to extract downloaded OpenVPN certificates from GUI. 21. 3G is not getting UP when WAN Mode is configured as Auto rollover with WAN3 as primary. 22. Unable to configure the IP aliasing entry on WAN2 interface. 23. Unable to support '/' (slash) character in Approved URLs and Blocked URLs page. 24. Unable to access GUI pages with IPV6 address of LAN. 25. Unable to Establish the PPTP and L2TP VPN tunnels with External authentication servers (Active Directory, NT Domain and LDAP Servers). 26. IPsec tunnel status do not update properly for Mobile phone. HQ20170222000011 27. CLI “show system log viewLogs” is not work. HQ20170606000001 28. Unable to enable multiple IPsec policy for identical remote network. HQ20170210000006 29. Unable to configure DNS server in IPsec tunnel mode. HQ20170510000003 30. Change max. value for NAT keep alive time to 3600. HQ20170531000020 31. Unable to allow TeamViewer when IP/IDP enable. HQ20170301000007 32. CVE-2014-0195, CVE-2014-0224, CVE-2016-2183, CVE-2014-3566 Vulnerability. HQ20170502000007 33. Captive portal can’t be triggered when the user doesn't add this particular VLAN. HQ20170119000011 34. Unable to establish IPSEC with AGGRESSIVE mode in behind NAT scenario. HQ20170511000003

3.11	1. Unable to edit Radio mode on Default wireless Profiles. [HQ20160615000005] 2. Unable to change the time zone after activating the WCF free trial license. [HQ20160819000002] 3. Unable to establish PPTP tunnel over PPPoE WAN with classical routing. [HQ20160830000012] 4. Device is showing Radio 1 or Radio 2 instead of 5.0 GHz or 2.4 GHz for connected clients in wireless clients page. [HQ20160919000010] 5. Able to configure 0.0.0.0 as IP address field in traffic selector setting page. [HQ20160922000014] 6. Unable to establish PPTP tunnel over PPPoE WAN. [HQ20161019000006] 7. Change the Severity of logs from error to Information for general platform logging. [HQ20161026000001] [HQ20161025000001] 8. Disallowing '/' (slash) character in Approved URL. [HQ20161025000011] 9. Unable to configure Radius server on WAN side for Radius Authentication. [HQ20161026000015] 10. DHCP relay functionality is not working in classical routing mode. [HQ20161025000002] 11. Web GUI is slow during logs generation when enable the logs. [HQ20161026000001] [HQ20160913000008] 12. Unable to access Web GUI in LAN site by using the WAN IP and URL. [HQ20161114000010] 13. Unable to change WAN mode, GUI shows 'A critical error encountered while loading web page'. [HQ20161026000003] 14. Unable to redirect to Https web page after Captive portal log in. [HQ20160926000006] 15. Unable to get WAN up for Russian dual access if Wan type is configured with Static IPs and server is configured with domain name. [HQ20161213000003] 16. Support all characters {excluding double quotes ("), back slash (\) and space characters} in PSK of IPsec policy from GUI and CLI. [HQ20161209000009] 17. WAN type PPPoE with “on demand” option is not work. 18. Support active private routes display in "IPv4 routes table in GUI". [HQ20150820000012] 19. WAN2 is unable to be standby again once WAN1 is reconnect in load balancing mode. [HQ20160622000010] 20. Unable to configure one VLAN ID on WAN1 and WAN2 both.

	[HQ20150420000008] 21. GUI display error for WiFi schedule control. [HQ20160616000013] 22. Custom NTP server is not syncing with Selected Timezone. [HQ20160616000012] 23. Unable to establish the PPTP and L2TP VPN tunnels when service route management enable. 24. Able to configure same name for server and client in OpenVPN certificate generation but unable to use in OpenVPN settings page. 25. Unable to save maximum PPTP/L2TP Client IP Range in Server side. 26. USB port is unable to access 2TB HDD. 27. Able to edit LAN DHCP reserved IPs entry by duplicate host name. 28. Huawei-E303 dongle is unable to get the Rollover WAN IP. 29. The configured DNS setting is able to override by ISP DNS server. [HQ20170119000012] 30. The logs is unable to refresh properly. 31. Unable to upload .csv file in Approved URLs page. 32. Rollover WAN is not getting UP after rollback to Rollover-WAN. 33. Unable to see SNMP v3 traps when entry added in SNMP Trap List. 34. IPV6 WAN2 functionality is not working [RU firmware] 35. Unable to set the date and time manually. [RU firmware] 36. Unable to capture the packets on DMZ interface. [RU firmware]
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 URIs priority is wrong. [DUSA20161014000002] 89. Unable to support DWM-157 B1 [DEUR20160913000002]

Known Issues:

Firmware Version	Known Issues
3.17	1. **OpenVPN Certificates Limitation**: Due to OpenVPN & SSL component upgrade, the old certificates generated/uploaded (in OpenVPN Certificates) are not compatible with the new OpenVPN component. Users either have to reconfigure (if custom certificates are being used or access server/client is chosen) or share updated default certificates to Clients (if default certificate is being used, as default certificate is updated) to be able to continue using OpenVPN.

Related Documentation:

- Unified Services Router User Manual v3.13
- Unified Services Router CLI Reference Guide v1.10