D-Link®

Unified Services Router Release Notes

Firmware Version:	2.02_WW
Published Date:	Aug. 3, 2015

Copyright © 2015

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

1

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. After firmware 1.04B58, new user database architecture is introduced. The new user database is easier to setup and more intuitively to use. When users upgrade DSR's firmware to 1.04B58 or later, DSR will automatically merge users in the old database into the new one. However, all new settings including new created users, firewall rules and application rules would be SWEPT AWAY and ONLY users, firewall rules and application rules being configured in the previous firmware will be kept when users downgrade firmware from 1.04B58 to the older one, e.g. 1.03B43. Please keep in mind: backup your configure file for further recovery once you decide to downgrade firmware to the older version.

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.

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 v2.02 User Manual*

New Features:

Firmware Version	New Features
2.02_WW	1. Brand New Web GUI design.
	2. SSL VPN supports external authentication database.
	3. Dynamic Web Content Filtering (subscription is required)
	4. Support DHCP ranges for all subnets.
	5. Support VLAN on WAN for single VLAN ID.
	6. Allow using a particular IP or VLAN to access GUI.
	7. Support more 3G USB dongles: add D-Link DWP-156 B1 and DWP-157 B1.
	8. OpenVPN enhancement: LAN subnet is accepted to be configured as the network of OpenVPN server.
	9. External HDD compatibility enhancement: Support up to 2 TB HDD.
1.09B61_WW	1. More 3G USB dongles support: add D-Link DWP-156 A1 and DWP-157 A1.
1.09B59_WW	None
1.09B38_WW	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. Bridge mode enhancements: support QoS and firewall rules.
	4. Spillover mode enhancements: both WAN1 and WAN2 will respond requests, e.g. ICMP, IPsec, etc., from Internet even when spillover threshold is not triggered.
	5. PPTP VPN enhancements: allow PPTP severs to assign remote clients the same subnet as the local LAN.
	6. Russia Dual Access enhancements: allow users to designate the outbound interface for IGMP control packets.
	7. Web GUI enhancements: support auto parameters fill-out in the DHCP server configuration page.
	8. CLI enhancements: support the "space" character.
	9. More 3G dongle supports: add D-Link DWM-156 A7, D-Link DWM-157 B1, and D-Link DWM-158 D1, HUAWEI E303.
	10. A new click button to quickly download Dbglogs.
	11. A new checkbox to enable/disable auto config backup.
	12. A new checkbox to enable/disable config file encryption.
	13. Support a Windows-based config viewer for encrypted config files.
1.08B88_WW	None
1.08B77_WW	None

dlink green

1.08B51_WW	1. Support more external Authentication server types for Captive Portal/SSL VPN/ IPSec user authentication. Available external authentication server types: NT domain, RADIUS, LDAP, AD and POP3.
	2. Support L2TP Client Mode: DSR can establish site-to-site L2TP tunnels to another DSR.
	3. Bandwidth Control enhancement: DSR can accept IP subnet for source IP addresses when configuring bandwidth management profiles
	4. Support GRE tunnels. Supported GRE tunnel numbers varies in different models - DSR-1000 series: 20; DSR-500 series: 15 ; DSR-250 series: 10; and DSR-150 series: 5.
	5. Support Layer 2 Bridge Mode: DSR can bridge DMZ (WAN2) with LAN port 1 in the Layer 2 level together.
	Note: Only DSR-500 and DSR-1000 series support Layer 2 bridge mode.
	6. Expand maximal IP-MAC binding (DHCP IP reserved) restrictions. Maximal numbers varies in different models - DSR-1000 series: 128; DSR-500 series: 96; DSR-250 series: 64; and DSR-150 series: 32.
	7. Support CAPWAP pass-through: DSR can recognize CAPWAP tunnel packets and allow them passing through LAN sides.
	8. Support D-Link DWM-157 A1 USB 3G modem.
	9. Increase IPSec pre-shared key length to 64 characters.
	10. IGMP enhancement: allow IGMP packets traversing DSR without specifying source IP addresses.
	11. Reduce Boot-up spent time.
	12. L2TP performance enhancement
1.06B53_WW	1. From firmware v1.06B53 and later, DSR-1000N, DSR-1000, DSR-500N and DSR-500 can support USB 3G modem which including D-Link DWM-152 A1/A2/A3, DWM-156 A1/A2/A3/A5/A6, Huawei E1550, E173 and EC306.
	Note: Only DSR-1000N and DSR-1000 can support to configure 3G USB modem as the 3rd WAN interface.
	2. Support VLAN functionalities on WAN interfaces.
	3. Support multilingual Web GUI through Package Manager. This solution is firmware independent which can easily check available language list through Internet by one click. After that, it can dynamically install/uninstall language pack.
	Note: only one language pack can be installed at a time in order to prevent consuming much Flash memory. Please remove the installed language before add any other language pack.
	4. USB 3G modem driver can be dynamically uninstalled/install through Package Manager.
	Note: Following 3G modem driver has already been built into firmware v1.06B53. D-Link DWM-152 A1/A2/A3, DWM-156 A1/A2/A3/A5/A6, Huawei E1550, E173 and EC306.
1.06B43_WW	1. Support basic OSPFv3 functionality on IPv4.
	2. New USB 3G dongles support: D-Link DWM-156 A5/A6, Huawei E1550, E173 and EC306. (DSR-1000N/1000 only)
	3. Support VLAN-based access control for USB Printer sharing and Storage Sharing.
	4. Support Russia dual access PPPoE.
	5. Support Wireless Distribution System (WDS). This feature is Only guaranteed to work between DSR routers of same model. For example, between two DSR-1000N, or between two DSR-500N. A max of 4 WDS peers can be

	specified, more detail please refer to the DSR user manual v1.05.
	Note: Using same firmware version between two DSR routers for WDS feature is strongly recommended.
	6. Firewall rules enhancement: support IPv6 firewall rules, allow users to select designate ports other than a sequent IP range, and allow users to select both TCP and UDP in one firewall rule.
	7. Support IGMP control package forwarding from WAN to LAN.
	8. Reduce WAN failover time to 1 minute.
	9. Support IPv4 DHCP relay through IPSec VPN tunnels.
	10. Support Captive Portal authentication through external RADIUS server.
	11. Allow both HTTP and HTTPS connections to the Captive Portal Login page.
	12. Support bandwidth management on the "inbound" traffic.
	13. Add a new option, threshold configuration, in the Block UDP flood settings.
	14. VPN failover. (DSR-500/500N/1000/1000N ONLY)
	15. Improve PPTP/L2TP performance.
	16. Allow to change MTU size for 3G connections.
	17. Extend IPSec Mode Config support to the following VPN clients: Netgear Prosafe VPN client (v5.02.001 or later), Greenbow VPN client (v4.65.003 or later) and Shrew Soft VPN client (v2.1.6 or later).
	18. WLAN scheduling improvement: Add a drop-menu called "Schedule control" with Turn-on and Turn-off options to control DSR WLAN ON/OFF.
1.04B58_WW	1. New IPv6 features include IPv6 over PPPoE and IPv6 prefix delegation.
	2. IPv6 web management enhancement.
	3. Support DHCPv6 leased-clients pages.
	4. User database management enhancement.
	5. Support policy based user database.
	6. Support policy based captive portal.
	7. Support PPTP VPN client mode: DSR could be a VPN client connecting to a PPTP server and share this PPTP tunnel with users behind DSR.
	8. Add new Internet settings, WAN3 setting: WAN3 interface is designated to 3G connections via USB dongles. (Available on DSR-1000/1000N only)
	9. Support SMS (Short Message Service) features. This feature is available when a USB 3G modem is connected to DSR router and 3G WAN interface is not configured as dedicated WAN mode or load balancing mode. Also, please make sure your service provider allow your SIM card to send/receive SMS through 3G network. (Available on DSR-1000/1000N only)
	10. Update CLI commands including VPN utilities CLI support.
	11. Enable classical and NAT routing option in PPTP server configuration.
	12. Support Firewall rules over VLAN.
	13. IPSec VPN enhancement: allowing users selecting multiple integrity, authentication and encryption method for phase1 & phase2 negotiations.
	14. Support a check box to block all URLs for Web site filtering feature. If users add some approved URLs, these URLs will be allowed.
	15. It's able to show logging message through CLI.
1.03B43_WW	1. Support SMTP ALG.
	2. Support full IPSec MIBs.
	3. OpenVPN enhancement – enabling gateway to gateway VPN tunnels.

1.03B36_WW	1. Intel AMT enhancements include Policy-based VPN configuration export for remote DSR router, AMT reflector modification, support DNS options for DHCP and DNS static host name mapping capability.
	2. Russia dual access PPTP/L2TP improvement.
	3. Support URL wildcard.
	4. Support to import/export a text or CSV file for keyword blocking. Keywords prevent access to websites that contain the specified characters in the URLs or the page contents.
	5. Built-in D-Link own certificate for SSL VPN code signing.
1.03B27_WW	1. Support WMM (Wi-Fi Multimedia) for DSR-500N and DSR-1000N.
	2. Support OpenVPN.
	3. Authentication and encryption method is modifiable in PPTP and L2TP.
	4. Support customized login page for captive portal.
	5. Captive Portal can take effective by different individual VLANs.
	6. Support private MIB for LEDs indicators of front panel.
1.03B23_WW	1. Support IKEv2.
	2. Support L2TP over IPSec.
	3. Support configuration auto-backup/auto-restore while a USB drive is inserted. Please refer to the implementation note for more detail of this document on page 2.
	4. Support SSL VPN CLI.
	5. Support Easy-Setup VPN feature. The benefit of this feature is that HQ IT/MIS can manually write a specific format file then deliver to non-IT background users of remote office. When the user imported this specific file in remote DSR router, all necessary VPN setting would be finished and ready for VPN tunnel establishment between HQ central site and remote offices.
	6. Support Intel AMT reflector.
1.03B12_WW	1. Support Non-Split tunnel for IPSec VPN.
	2. Support USB storage and printer sharing.
	3. Improve WAN configuration page based on drop-down menu.
	4. Support logging for SSL VPN activity.
	5. Support Interoperability with Cisco VPN client in iPhone OS4.
	6. Support NAT hair-pinning.
	7. Reverse the logs display, so that the latest logs are shown at the top of the viewer.
	8. Support DWM-152/156 A3 3G USB dongle. (This only affects in DSR-1000/1000N)
	9. Support for enable / disable Jumbo frames.
	10. Support for add / edit / delete routing table of secondary PPPoE tunnel.
	11. Spill over mode improvements - configurable maximum WAN bandwidth and load tolerance.
	12. Support captive portal.
	13. Support Blowfish and CAST-128 encryption-authentication algorithms in IKE Policy Configuration page.
	14. Support for IPSec policy option for AH alone (without ESP)
	15. Support for temporary blocking of user login for brute password attack.

	16. Available to choose the local traffic selector in VPN Wizard page.
1.02B25_WW	1. Added support for Russia PPTP/L2TP Dual Access.
	2. Support IPSec Failover
	3. Support for DWM-152/156 A1/A2 3G USB dongles with firmware 1.03 and 1.05
	4. Added support for RFC 3442 for DHCP client
1.02B11	SSL VPN module upgrade to support SSL VPN on Windows 7 and Mac 10.6 operating systems
1.01B50	It's the first release.

Changes of MIB & D-View Module:

DSR series can support LED MIB from firmware v1.03B27 and later.

Problems Fixed:

Firmware Version	Problems Fixed
2.02_WW	1. Fix Port forwarding (HTTPS/PPTP) issue. **(DEUR20140626000004)**
	2. Two windows wireless clients can't ping to each other when the security mode is configured as WPA/WPA2/WPA+WPA2 **(DRU20140826000002)**
	3. Help content enhancement: WAN IP address should not be configured as primary/secondary DNS server IP address. **(DLA20140619000005)**
	4. Will not accept to install the CA certificate without common name. **(DEUR20140623000007)**
	5. Fix WAN port speed issue with Cirrus CPE. **(DI20140307000005)**
	6. Fix unable to import the blocked keywords and approved URL csv files which are exported by DSR. **(DRU20140709000004)**
	7. The PPTP client can't access to LAN PC when all traffic is bound to a specific WAN port with protocol binding. **(DEUR20140617000001)**
	8. Fix the issue that HTTP server can see the internal IP of DMZ instead of external IP. **(DEUR20140714000008)**
	9. Fix unable to configure DSR as OpenVPN server with firmware version 1.09. **(DEUR20140729000007, DI20140804000004)**
	10. CLI issue: Does not accept valid CIDR subnet mask via CLI. **(DI20140618000001)**
	11. Fix unable to set the firewall rules with the same service but different schedules. **(DRU20140521000004)**

	12. Fix missing TOS bits issue when using VLAN and QoS in the WAN port. **(DLA20140619000005)**
	13. Fix known issue: voice at LAN side client is not heard when the SIP Proxy resides in LAN.
	14. Wireless TCP receive side throughput performance with Veriwave is not good (IxChariot & over-the-air is OK).
	15. Fix PPTP pass through taking highest priority than PPTP firewall service.
	16. Fix IPSEC pass through taking highest priority than IKE outbound firewall service.
	17. Fix the issue opening LAN clients page takes too long time.
	18. Fix known issue: Blank field for "data to supply to CA" when click view button in Self certificates requests page.
	19. Multicast traffic can't go smoothly on the wireless of DSR. **(DRU20110426000001)**
	20. Fix known issue: device keeps sending log to syslog server after the configuration of server IP address is removed.
	21. Fix mismatch between configured and displayed transmit power.
	22. Fix known issue: transparent mode doesn't work on WAN2.
	23. Fix known issue: USB storage issue with Windows XP.
	24. Add the description about 'Response to Ping' in the help page of PPTP and L2TP servers.
	25. Fix known issue: IPSec tunnel can't be established when the configuration file which is exported from another device is imported.
	26. Fix Unstable WLAN issue. **(DEUR20120611000010, DEUR20120718000007, DEUR20120905000005)**
	27. Fix firewall rule by schedule issue. **(DRU20140521000004)**
1.09B61_WW	1. Captive portal support an option, administrator can allow/disallow "password change" for captive portal users.
	2. DDNS feature can work properly when DSR is deployed behind NAT router.
	3. **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 **Solution:** Patched OpenSSL to 0.9.8za
	4. Improve CLI command to change multiple SSIDs with specific VLAN.

		(DGC20140506000001)
		5. Fix bandwidth control issue (DEUR20140423000001)
		6. Fix the issue to enable Invalid ICMP Packet log via CLI command. (DI20140516000003)
		7. Fix unable to configure domain name of DHCP server as blank via CLI command. (DI20140516000003)
		8. Fix the exporting blocked keyword issue. (DRU20140521000001)
		9. Fix uPnP feature is not working properly. (DEUR20140505000003)
		10. Fix Dyndns update fail when WAN is set to failover mode. (DI20140521000005)
		11. Fix service name "Any" missing in Web GUI. (DI20140521000003)
1.09B59_WW		1. Users can't save WDS settings after enabling WDS. (DRU20140212000003)
		2. Removing debug messages from general console logs. (DI20140110000001)
		3. After enabling "Enable Remote SSH" in the remote management setting page, users can't login DSR Web GUI from the WAN interface. (DEUR20140117000002)
		4. When both WAN1 and WAN2 are working in the classical routing mode, DSR shouldn't force users to configure an internal IP address in destination NAT settings. (DGC20140115000001)
		5. When users set a static IP address for Russia Dual Access L2TP WAN connections, DSR can't establish Internet connections with ISP. (DRU20140331000009)
		6. Even when users disable inter-VLAN routing in the VLAN setting page, users under the default VLAN, i.e. VLAN1, still are able to ping users under other VLANs. (DEUR20140320000003)
		7. When Regional characters, e.g. Kanji, are used in a user name, DSR would fail to store this kind of user names in the local database. We'll restrict users to only use English characters or numbers in a user name. (DI20140116000006)
		8. There is a feature, VLAN on WAN support, missing in the previous formal release. (DI20140416000004)
		9. More accurate progress as well as more execution information for firmware upgrade.
1.09B38_WW		1. WAN failure detection issues: DSR can't allow using a ping-detecting

		server that is not in the same subnet as gateway. **(DEUR20121116000011)**
	2.	After delete IPsec one to one mapping rule, it could not drop the IPsec tunnel from DSR Web GUI.
	3.	After delete the IPsec one to one mapping rule, local PC is still able to ping remote PC with mapping IP address.
	4.	While changing the local network in IPsec policy, web GUI will display incorrect message.
	5.	The CLI: *security firewall ipv6 configure/edit* doesn't work.
1.08B88_WW	1.	Fix DSR cannot edit the VLAN via CLI when it has the max VLAN.
	2.	Fix one-to-one LAN NAT issue **(DI20130704000001)**
	3.	Custom services port type: multiple ports, won't work when used in firewall rule with port forwarding **(DEUR20131028000008)**
	4.	Fix DSR shows incorrect SNMP information **(DEUR20130529000002)**
	5.	Fix device sporadic hard reboot issue **(DEUR20130813000001)**
	6.	Fix DSR cannot send itself traffic through IPsec site-to-site VPN tunnel **(DEUR20130826000006)**
	7.	Fix WAN1/WAN2 port status and counters issue **(DEUR20131016000004)**
	8.	Fix Wi-Fi 5GHz frequency channel list incorrect issue for TW and RU region. (DSR-1000N only)
	9.	Fix CLI command "show net statistics all" does not include information related to WAN2 interface.
	10.	CLI command "show net wan port_setup" doesn't display actual interface link speed.
	11.	Update DSR's online help information for IPsec one to one mapping.
	12.	Fix IPsec failover cannot roll back issue. **(DRU20131111000004)**
	13.	Fix following CLI doesn't work. *security firewall ipv6 default_outbound_policy* *security firewall ipv6 delete <row_id>* *security firewall ipv6 disable <row_id>* *security firewall ipv6 enable <rowd_id>*
1.08B77_WW	1.	**Security Vulnerabilities Addressed:** devices respond clients some unnecessary information, and hence give hackers a chance to hack devices. **Reference:** CVE-2013-5945, CVE-2013-5946 **Solution:** Remove all unnecessary root user accounts.

2. **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.

3. Dual WAN issues: clients can't get ICMP responses from WAN interfaces when both WAN are linking up. **(DGC20130203000001)**

4. Dual WAN issues: remote clients can establish PPTP tunnels to WAN1 but fail to establish PPTP tunnels to WAN2 when dual wan are active. **(DEUR20130313000009)**

5. IPSec issues: When Netbios is enabled in a IPSec policy, Netbios enabled clients are unable to open share folders of LAN hosts with Netbios name. **(DUSA20130206000001)**

6. IPSec issues: in some situations, IPSec tunnels got disconnected sporadically, and can't recover quickly. **(DI20130325000007)**

7. IPSec issues: devices don't send DPD-R-U messages regularly based on the user configurable interval. **(DRU20130726000001)**

8. PPTP issues: clients can't establish PPTP tunnels to devices when using external LDAP servers for user authentication. **(DEUR20130412000004)**

9. L2TP issues: devices would keep l2tp sessions active even when wan connections link down. **(DRU20130718000002)**

10. Certificate issues: unable to delete the trusted CA from the Advanced->Certificates page. **(DEUR20130507000002)**

11. DMZ issues: WAN3 and DMZ can't be activated simultaneously. **(DLA20130429000001, DLA20130704000004)**

12. DHCP issues: DHCP relay can't work between LAN and VLAN. **(DRU20130723000005)**

13. Log issues: device can't save 1,600 logs in the record, and logs with the same time stamp can't be observed in the top or bottom in the all logs page. **(DI20130108000002)**

14. Online help issues: descriptions of blocked keyword are not correct. **(DEUR20130201000002)**

15. CLI issues: unable to use space in the group description. **(DI20120828000009)**

	16. CLI issues: can't set SSL VPN banner messages in CLI. (DI20120831000003)
	17. GUI issues: the radio channel still shows 2.4GHz after admin change the WiFi Operating Frequency to 5GHz. (DI20121101000003)
	18. Others: ICMP traffics to remote IPSec clients will be blocked if admin sets Default Outbound Policy as "Block Always". (DRU20121023000003)
1.08B51_WW	1. IPSec passthrough is not working for wireless clients.
	2. Multiple LAN users are able to access Internet using single captive portal account at the same time.
	3. Unable to play counter strike online from wireless clients.
	4. L2TP dialup can't allow pure numbers using in password and username.
	5. Unable to enable DMZ via CLI.
	6. PPTP/L2TP clients can't ping LAN clients under VLAN ID that is greater 10.
	7. Unable to add SSL VPN policy via CLI.
	8. Unable to check the status of SSL VPN tunnels via CLI.
	9. PPTP ALG is not working
	10. Device don't send DHCP-request messages after the end of T1 lease time (0.5*lease time).
	11. DWM-156 A3 is not working properly.
	12. When using management tools, traceroute, the first hop shows destination IP rather than router IP.
	13. Authenticated clients are redirected to the captive portal logout page while authenticated clients are trying to access Internet.
	14. Device allows LAN DHCP server range to overlap with sslvpn client address range.
	15. Unable to configure the "date and time" filed in the date and time page from CLI.
	16. Unable to configure IPSec policy in transport mode from CLI.
	17. While users copy a file over 600MB from Windows 7 LAN host to the USB drive, error messages will be popout.
	18. LAN clients information don't show correctly in the 'LAN clients' page.
	19. EPSON Stylus Photo 830 printer shows different model names in GUI and Back-end.
	20. Device doesn't synchronize with correct time in different time zones. Also, device' time is still persisting after factory default.
	21. After firmware upgrade, configured IPSec policy has be changed.
	22. Device doesn't accept '0.0.0.0' in the IP address and subnet mask field in SNMP access control list page.

dlink green

23. Device displays the error messages, 'i18nhtmlmissing', in the GUI while users try to disable "enable redundant policy" option in the primary policy.

24. DWM-156 A6 dongle is not working as 3rd/backup WAN.

25. DWM 156 A3 3G dongle is not mounted properly in some cases.

26. **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.

27. In some rare cases, device displays the error messages, 'i18nhtmlmissing', in the GUI while users try to disable "DHCP under VLAN".

28. Device shows miss-match authentication and encryption methods in the IPSec backup policy.

29. Device shows some meaningless messages in the logs.

30. Device can't accept remote IPSec endpoint as FQDN 0.0.0.0.

31. PPTP clients can access LAN networks but fail to access other VLAN networks.

32. "DNS request timeout" is observed in windows lan host while doing nslookup when iIPS/IDP is enabled in the device.

33. Clients' LAN-to-WAN traffics are redirected to http server on the lan side when inbound (WAN-to LAN) HTTP rules are added on WAN3.

34. Device doesn't show the WiFi current channel in the "Radio Settings" page and "WLAN Status" page when the default AP is disabled.

35. Removing some RD debug/meaningless logs.

36. CLI issues: 1. there is no commands to select VLAN,DMZ and WAN3 interfaces for packet capturing. 2. Fail to change the file name saving the captured packets.

37. DDNS is not updating the WAN IP address after disabling and enabling the DDNS functionality from the WAN status page.

38. The 26th PPTP user in the database can't establish the PPTP tunnel to DSR even if the PPTP tunnel limitation is not reached.

39. Unable to establish PPTP/L2TP tunnels if PPTP/L2TP clients' username or password includes "#" character.

40. X.509 Cert for SSL VPN Tunnels is expired.

41. There is no 3G information available in the dashboard page to show statics.

42. DSR-1000(N) is unable to show 1600 log entries in the view logs page.

	43. The Captive Portal Setup page shows the default profile as "In Use" without adding any captive portal policy.
	44. Device can't connect to ISP using L2TP if the username or password of a L2TP accounts starts with 0, e.g. 01234.
	45. Active sessions page doesn't show any entry for active sessions.
1.06B53_WW	1. Some 3G dongles are displayed incorrect device model name in the USB setting page.
	2. PPTP client mode fails to support the MPPE 40bits encryption method.
	3. WiFi channel list shows incorrect wireless channels.
1.06B43_WW	1. Reserved IP should be outside of the DHCP IP pool range: a user will not be allowed assign a static IP that is in the DHCP IP pool.
	2. Spillover is not working between PPPoE.
	3. PPTP compatibility issues with Android phones in the encryption mode.
	4. Need to remove "ANY" Service from Bandwidth traffic selectors services options: to avoid users' confusion when configuring bandwidth control.
	5. Dash board show blank page after running heavy traffic.
	6. LAN side VLC Receiver does not receive multicast traffic from VLC sender.
	7. Firewall has the highest priority than content filtering ->approved URL: Now white/black list owns the highest priority.
	8. Unable to send the Email logs to the SMTP server present in LAN side of the device.
	9. DSR web GUI can't be accessed remotely through tunnel.
	10. Device is still using old certificates to access the web GUI after uploading new VeriSign-signed certificates.
	11. Unable to do NetBIOS from PPTP and L2TP Clients.
	12. LAN reserved IP's page got missed in I.E browsers if we set IE's languages to French.
	13. PPTP connection is using MAC of WAN PHYs as gateway.
	14. Fail to save and configure IP addresses via CLI.
	15. When Inter-VLAN is disabled, clients still can access the WEB GUI and USB disk by using IP addresses in another VLAN.
	17. Support User-FQDN in IPSec policies.
	18. IP Aliasing causes errors when user configures Firewall rules without specifying host range.
	19. IP/MAC binding is not associated with DHCP reserved IP addresses.
	20. Skype can't login through WIFI.
	21. Fail to auto-rollover to 3G dongle when it is configured as WAN2.

	22. IGMP control packet forwarding issue: LAN side VLC Receiver does not receive multicast traffic from VLC sender when DUT is behind NAT router.
	23. Compatibility issue between DSR devices and Android PPTP clients when enable encryption' is enabled in Both devices.
	24. Firewall has the higher priority than approved URL specified in content filtering.
	25. Fail to PING DNS server after fail-over to backup WAN2.
	26. During failover period, private LAN IP addresses will appear on the WAN side.
	27. DSR never reconnects to L2TP server after soft-reboot.
	28. In Windows environments, Google mail/Thunderbird client can't attach file size over 4MB.
	29. User can't configure static routes VLAN interface through CLI.
	30. There are some incorrect statements in DSR WAN mode help.
	31. Unable to register sip client in android phone to the sip server over internet through the device.
	32. Device displays ""1i8nHTML missing"" messages while users try to configure the optional port to DMZ.
	33. LAN ports may be shut off when users import some special configuration files.
1.04B58_WW	1. User not able to add static route for sit0 tunnel with 6 to 4 gateway address from CLI.
	2. Unable to add custom services from CLI.
	3. Unable to login in MSN messengers (windows live messenger-2011) from PPTP client (windows-7) through PPTP server is enable in DSR-1000N.
	4. Device giving critical error when user tries to delete the added user.
	5. IPv6 gateway has address restrictions, i.e. sit interface first octet with > 25 and < 100.
	6. String can be input "space" letter in SSL VPN custom portal layout name, title and banner field.
	7. Improved WAN failover time.
	8. DHCP reserved IP addresses doesn't work.
	9. Dashboard page would show a blank page.
	10. Sometimes, the DNS resolving would stop around 1 minute.
	11. Compatible issues with the native PPTP client in Android 2.2.
	12. IGMP proxy only works on one direction (WAN-to-LAN).
	13. PPPoE performance is limited below 50Mbps.
	14. Login policies are not working for Admin and Guest users.

	15. When trying to delete a new created user immediately, DSR would pop out an error message: A critical error encountered while loading web page. 16. Fix DSR router is hard to get IP address from D-Link DSL-320LB modem. 17. Fix Ping and DNS WAN failure detection method not following configured intervals. 18. Fix Rollover feature doesn't work when the WAN2 is configured to 3G networks. 19. Fix file name will be garbled if naming is Chinese Traditional in USB Disk. 20. While accessing PDF files or picture files via DSR-500N USB sharing in Windows 7 64-bit machines, Windows 7 is crashed and blue screen is coming. 21. PPPoE performance improvement.
1.03B43_WW	1. Fix WPS paring issues with DCS-930L camera. 2. Fix PPTP tunnel issues – PPTP server would keep the same IP when LAN and PPTP server are in the same subnet. 3. VPN setting enhancement – remove character length limitation for SA identifier. 4. Fix incorrect responses when typing CLI commands "show security firewall ipv6 setup" 5. Fix captive portal login page cannot show correctly on the iPhone/iPad. 6. Fix LED incorrect behavior when configuring 5GHz band for DSR-1000N.
1.03B36_WW	1. Intel AMT cannot get default route from the built-in DHCP Server. 2. PPTP SYN packet is going with DHCP server MAC address. 3. Fix the interface IP address should be 172.17.100.254/24 by default when WAN2 port is configured as DMZ. 4. It's not able access the Intel AMT client located at LAN side from Intel AMT server at WAN side after turned off the Intel AMT. 5. It's not able to send FTP and HTTP traffic through IPSEC VPN tunnel between DSR-1000N and DSR-500N.
1.03B27_WW	1. Fix USB Storage sharing is accessible from WAN. 2. Device blocking DMZ to WAN traffic when captive portal authentication is enabled on default VLAN(LAN). 3. Captive Portal feature will block users accessing internet through IPSEC VPN and SSL VPN tunnel. 4. CLI is prompting for prefix in ipv4 static routing configuration. 5. User is unable to set the exchange mode as Aggressive using CLI while adding IPSec VPN policy.

	6. User able to add group based SSL VPN policy for not existed group from CLI.
	7. Device is accepting the SSL VPN Client IP address range which is in the LAN subnet from CLI.
	8. IKEv2 is unable to establish the tunnel when WAN cable unplug and plug it back.
	9. It's not able to establish VPN tunnel with Extended Authentication as Edge device using Easy-Setup VPN import file.
	10. After delete same self certificate and reboot, device is not showing error message while deleting CA cert.
	11. The Java console of SSL VPN client is showing DES as cipher suite for SSL VPN tunnel.
	12. Observed critical error in browser login page when user entered URL "https://<LAN IP>/scgi-bin/platform.cgi/".
	13. Need to update User Policy By Client Browser with IE, Firefox, Opera and Chrome" only.
	14. Device is not throwing correct error message when user login wrong portal name.
	15. Need to restrict the WebUI access using remote management port from LAN side.
	16. It's able to change the default domain, group and user configuration through CLI.
	17. Current Web GUI session of logged in user is not terminating after changing password through CLI.
	18. IKEv2 Traffic Selector Type: Range is not supporting.
	19. PPTP Server have no option to disable MPPE encryption.
	20. Need to change help content in DMZ page.
	21. Device is not showing portal layout URL IP address as "0.0.0.0".
1.03B23_WW	1. Problem routing TCP traffic in VPN tunnel.
	2. USB printer sharing will not work after manually reboot.
	3. Inbound Intel AMT feature is not working in load balancing mode.
	4. It's not able to block ICMP traffic using SSL VPN policy.
1.03B12_WW	1. Device displaying local server IP in GUI after changing the firewall rules from allow always to block always.
	2. Device not displaying "Local1-UTM" option at SysLog Facility options in remote logging configuration page.
	3. Improve Japanese Multiple PPPoE usability issue.
	4. Manually Configured "Use These DNS Server", DNS is not updating for

	PPPoE/Japanese multiple PPPoE ISPs.
	5. Block user access to Captive Portal login page, when Captive Portal is disabled.
	6. Adding USB storage and Printer help pages.
	7. USB1 status not being updated dynamically.
	8. Print jobs are not being deleted after the print is done.
	9. User is able to upload more than one active self cert in Authentication page causing "critical error" in linux firefox and blank page in "opera".
	10. USB storage does not work after reboot.
	11. Fixed firewall dependencies on USB storage and Printer.
	12. Able to access the data from Linux host even after clicking 'Safely Removed' button for USB storage.
	13. Increase range for retry interval of WAN failover between 5 to 999 seconds.
	14. Observed kernel dump due to unaligned memory access while removing the 3G USB dongle (unmounted incorrectly)
	15. WEP key doesn't support ASCII. (This only affects wireless models)
	16. Duplicate domain names are showing in domain drop down if users add custom group in group pages.
	17. Device does not send DHCP release to DHCP server (after soft reboot).
	18. Error message displayed and redirected to add VLAN page on checking the Inter VLAN Routing button in default VLAN.
	19. Device is not accepting more than 15 characters in 'Server address' field in WAN1 setup page.
	20. SSL VPN performance optimizations.
	21. It's not able to establish Gateway-to-Gateway IPSec VPN with Phase 2 encryption algorithm as "None".
	22. 'Default admin user' session is getting terminated after login to the DUT with 'custom admin user' from LAN/WAN side.
	23. It fails to import CSV file of DOS format.
	24. Sometimes 3G network is not connecting when plug-out & plug-in the card multiple times.
	25. Update Help Pages for WAN configuration pages.
1.02B25_WW	1. Current guest session is not logging out even if we change the password using admin account from same/different host.
	2. Change the "Enter Your Password" field as "Enter Current Logged in Administrator Password" in edit users page.
	3. Able to add protocol binding rule for same service on all WANs in load

balancing mode.

4. DHCP relay issues when user configures more than 4 VLANS to DHCP relay.

5. Router is not accepting local/remote traffic selector IP with 4th octet value as other than '0' (zero).

6. User able to configure Primary and secondary wan with same pptp/l2tp credentials.

7. Clone your MAC address option doesn't work for WAN2.

8. Need to add validation in Approved URL page.

9. After enabling all logging options and device name with max special characters, if user changes the lan subnet then it won't reflect in GUI and backend.

10. User is able to configure the WAN1/WAN2/DMZ ip address as loop back (127.0.0.1) address.

11. Error message displayed and redirected to add vlan page on checking the Inter-VLAN routing button in default VLAN.

12. DUT is accepting more than 64 characters at Username, Domain name and Password fields in Dynamic DNS page.

13. Observed critical error in WebUI after manually removing USB and if user tries to refresh the browser.

14. User not able to enable WPS for WPA and WPA2 security mode and "wsccmd" processes in Zombie state while enabling the WPS.

15. Device is not showing ipv6 gateway IP in Device status page.

16. Device is throwing wrong error message while adding an entry without any name in IP/MAC binding configuration page.

17. Device is accepting duplicate IP and MAC entries in IP/MAC binding configuration page.

18. In static routes for Ipv6. Subnet validation is not happening for routes with interface as Wan2.

19. User should not able to configure PPTP/L2TP server's Starting IP Address and Ending IP Address in the subnet of LAN/VLAN/DMZ.

20. Dash board GUI issues in different browsers with multiple applications when we select different interface in Russia image.

21. Support Maximum characters limit check for Names fields In Users, Domains , Groups pages,SSL Resources,SSL Portforwarding.

22. Device Displaying "Specified portal not found" when configure portal layout name with maximum special and legal characters

23. Device is sending the DPD packets to the remote wan of VPN gateway after

	every 5 seconds. 24. Device showing "null" in wan connection status when no cable connected to interface and wan mode in idle. 25. DSR-500N default channel is changed to 6. 26. if SSL username contains special characters, Device displaying white blank page instead of client portal page. 27. Generate self certificate request should have signature key length 2048 bits 28. Portforwarding tunnel not establishing in java based browsers. 29. While establishing SSL VPN, Strongest cipher suit selection is desired from SSL server. 30. USB settings page not showing correct status for 3G Device exposing LAN host IP as terminator: in remote login page
1.02B11	1. Same SSID can be configured for two different APs (should be prevented) 2. Domain name is not coming with asterisk sign(*), if we made custom portal as default. 3. Duplicate domain names are showing in domain drop down if we add custom group in group pages. 4. Scalability Issue - Admin can add more than maximum users limit. 5. Displaying html code in GUI page when user tries configure pppoe profile with all special characters. 6. Need IP address validation in NTP page. 7. Device not displaying vlan's lease information in DHCP leased clients page. 8. Device not displaying correct IPV6 DNS information in Device status page. 9. Primary and secondary DNS server fields in LAN IPv6 page are not grayed out when user select "Use DNS from ISP" option. 10. When VLAN is disabled, other options in VLAN pages are not grayed out. 11. SSL External Authentication with LDAP is not working. 12. LAN's IPv6 address is getting configured wrongly. 13. Changing LAN IP doesn't restart DHCP server. 14. Issue with port '0' in custom service. 15. RDP or VNC over load balancing (incoming) is not working after 30+ min. 16. Crash with ixChariot heavy traffic + USB continuous read/write operations (simulate full load DVT testing) and also observed kernel dump when runnning traffic between WLAN clients. 17. Device not displaying device statistics when wan connected with PPP link. 18. SSLVPN tunnel getting dropped in 3 minutes with Linux OS.

	19. Observed unknown WINS server and DNS server information while connecting L2TP client to DSR1000N router as L2TP server. 20. Without sending terminal-request packet when L2TP tunnel manually disconnected. 21. Device taking around 90 seconds login after factory reset from GUI. 22. DWA-160 can't connect to DSR-1000N with WPS. 23. WAN2's IPv6 address is empty in GUI. 24. User not able to add the multiple set of source and destination users in firewall page. 25. When WAN1 is configured as L2TP and WAN2 is configured as any link types, Auto-Failover is not working with failure detection method with Default/Custom DNS. 26. WiFi Clients are not associating to AP when Pre-authentication is enable. 27. In all auto refresh pages, Device showing 5 seconds instead of 10 seconds after user tries to configure invalid pool interval time. 28. No validations for ISATAP subnet prefix in ISATAP Tunnels page. 29. "Display the IPv6 Routing Table" should grayed out in IPV4 mode. 30. Wan mode switching (WAN1 <=> WAN2) is not reflecting at backend. 31. WiFi frequency is not changing from 2.4 GHz to 5 GHz when using CLI
1.01B50	1. Device displaying inaccurate error message like "SSL-VPN client pool is also in the same range. Please configure different IP." When user configure the LAN DHCP server page with alphabets "abc.cde.fgh.ijk". 2. Device allows user to configure other special characters in primary/secondary NTP server fields. 3. Device displaying wrong error message while uploading Firmware via USB page without selecting any file. 4. After configuring resource for subnet, if user add the single IP address, device displaying the previous IP network subnet mask in GUI. 5. User should not be able to configure the SSLVPN client LCP time out as "0". 6. Look GUI and feel issue when "help" is clicked in SSLVPN portal pages. 7. Validation needed for IPv6 Advertisement prefixes page. 8. The USB page shows wrong icons initially for an instant, then displays correct icons. 9. WAN is not coming up automatically if cable removed before upgrade from B42 to B48, user must enable WAN from GUI. 10. DUT can't reset to default. Wireless client not disconnect from DUT when push the reset button. 11. Wireless DHCP clients can't get correct IP address from VLAN.

Bug fixes having been scheduled into the next release:

Firmware Version	Reported Issues
Next Release	None

Known Issues:

Firmware Version	Known Issues
2.02_WW	1. In the WAN spill-over mode, DSR don't allow users to establish L2TP and L2TP over IPsec from Internet to WAN 2 when WAN 2 is not triggered to be active. 2. There is an issue where the router is not able to transfer files > 250MB from Windows XP to USB storage after apply WinXP.reg script file. 3. Daylight saving with manual settings is not working properly for Newfoundland and Greenland time zones. 4. It's able to configure the same MAC address to WAN1 and WAN2 ports by selecting the 'Clone your PC's MAC Address' option. 5. After editing the WEP profile (wep-64), another WEP profile (wep-128) wireless client is not reconnecting until disable/enable the corresponding SSID. 6. VLAN dropped in and dropped out packet entries are incorrect in dashboard page. 7. User cannot enable UPnP on LAN and VLAN simultaneously. 8. Bandwidth rules over IPsec VPN tunnel are not being followed. 9. Snmpwalk takes long time to display IPsec details. 10. Spillover threshold can't approach configured value very precisely. 11. IPsec failover only works for specific scenarios, e.g. in site-to-site tunnel mode, IPsec failover will only happen in one of end points. 12. Bandwidth control does not work when users select pre-defined services, e.g. http or "ftp. 13. Specific Service support for inbound traffic management is not work.
1.09B61_WW	1. In the WAN spill-over mode, DSR don't allow users to establish L2TP and L2TP over IPsec from Internet to WAN 2 when WAN 2 is not triggered to be active. 2. When wireless clients paly multicast HD streaming, WAN performance will

be seriously impacted.

3. Transparent mode is only working on WAN1.

4. There is an issue where the router is not able to transfer files > 250MB from Windows XP to USB storage after apply WinXP.reg script file.

5. Voice at LAN side client is not heard when the SIP Proxy resides in LAN.

6. Daylight saving with manual settings is not working properly for Newfoundland and Greenland time zones.

7. It's able to configure the same MAC address to WAN1 and WAN2 ports by selecting the 'Clone your PC's MAC Address' option.

8. After editing the WEP profile (wep-64), another WEP profile (wep-128) wireless client is not reconnecting until disable/enable the corresponding SSID.

9. Blank field for "data to supply to CA" when click view button in Self certificates requests page.

10. VLAN dropped in and dropped out packet entries are incorrect in dashboard page.

11. User cannot enable UPnP on LAN and VLAN simultaneously.

12. Bandwidth rules over IPsec VPN tunnel are not being followed.

13. Device keeps sending syslogs to syslog server after removing the earlier configured syslog server IP address.

14. USB storage is not working perfectly with windows XP. It's not able to open files without copying them locally and it has issue to copy larger files from Network Storage share on to the Windows XP host.
(Note: 1. Copy files from Windows XP to Network Storage works fine. 2. This issue doesn't affect Windows Vista, Windows 7 and Linux based operating systems)

15. IPSEC tunnel is not getting established after importing the exported file at the remote device until disable then enabling policy

16. Snmpwalk takes long time to display IPsec details.

17. Spillover threshold can't approach configured value very precisely.

18. IPsec failover only works for specific scenarios, e.g. in site-to-site tunnel mode, IPsec failover will only happen in one of end points.

19. Bandwidth control does not work when users select pre-defined services, e.g. http or "ftp.

20. Specific Service support for inbound traffic management is not work.

| 1.09B59_WW | 1. In the WAN spill-over mode, DSR don't allow users to establish L2TP and L2TP over IPsec from Internet to WAN 2 when WAN 2 is not triggered to be active. |

2. When wireless clients paly multicast HD streaming, WAN performance will be seriously impacted.

3. Transparent mode is only working on WAN1.

4. There is an issue where the router is not able to transfer files > 250MB from Windows XP to USB storage after apply WinXP.reg script file.

5. Voice at LAN side client is not heard when the SIP Proxy resides in LAN.

6. Daylight saving with manual settings is not working properly for Newfoundland and Greenland time zones.

7. It's able to configure the same MAC address to WAN1 and WAN2 ports by selecting the 'Clone your PC's MAC Address' option.

8. After editing the WEP profile (wep-64), another WEP profile (wep-128) wireless client is not reconnecting until disable/enable the corresponding SSID.

9. Blank field for "data to supply to CA" when click view button in Self certificates requests page.

10. VLAN dropped in and dropped out packet entries are incorrect in dashboard page.

11. User cannot enable UPnP on LAN and VLAN simultaneously.

12. Bandwidth rules over IPsec VPN tunnel are not being followed.

13. Device keeps sending syslogs to syslog server after removing the earlier configured syslog server IP address.

14. USB storage is not working perfectly with windows XP. It's not able to open files without copying them locally and it has issue to copy larger files from Network Storage share on to the Windows XP host.
(Note: 1. Copy files from Windows XP to Network Storage works fine. 2. This issue doesn't affect Windows Vista, Windows 7 and Linux based operating systems)

15. IPSEC tunnel is not getting established after importing the exported file at the remote device until disable then enabling policy

16. Snmpwalk takes long time to display IPsec details.

17. Spillover threshold can't approach configured value very precisely.

18. IPsec failover only works for specific scenarios, e.g. in site-to-site tunnel mode, IPsec failover will only happen in one of end points.

19. Bandwidth control does not work when users select pre-defined services, e.g. http or "ftp.

20. Specific Service support for inbound traffic management is not work.

| 1.09B38_WW | 1. In the WAN spill-over mode, DSR don't allow users to establish L2TP and L2TP over IPsec from Internet to WAN 2 when WAN 2 is not triggered to |

be active.

2. When wireless clients paly multicast HD streaming, WAN performance will be seriously impacted.

3. Transparent mode is only working on WAN1.

4. There is an issue where the router is not able to transfer files > 250MB from Windows XP to USB storage after apply WinXP.reg script file.

5. Voice at LAN side client is not heard when the SIP Proxy resides in LAN.

6. Daylight saving with manual settings is not working properly for Newfoundland and Greenland time zones.

7. It's able to configure the same MAC address to WAN1 and WAN2 ports by selecting the 'Clone your PC's MAC Address' option.

8. After editing the WEP profile (wep-64), another WEP profile (wep-128) wireless client is not reconnecting until disable/enable the corresponding SSID.

9. Blank field for "data to supply to CA" when click view button in Self certificates requests page.

10. VLAN dropped in and dropped out packet entries are incorrect in dashboard page.

11. User cannot enable UPnP on LAN and VLAN simultaneously.

12. Bandwidth rules over IPsec VPN tunnel are not being followed.

13. Device keeps sending syslogs to syslog server after removing the earlier configured syslog server IP address.

14. USB storage is not working perfectly with windows XP. It's not able to open files without copying them locally and it has issue to copy larger files from Network Storage share on to the Windows XP host.
(Note: 1. Copy files from Windows XP to Network Storage works fine. 2. This issue doesn't affect Windows Vista, Windows 7 and Linux based operating systems)

15. IPSEC tunnel is not getting established after importing the exported file at the remote device until disable then enabling policy

16. Snmpwalk takes long time to display IPsec details.

17. Spillover threshold can't approach configured value very precisely.

18. IPsec failover only works for specific scenarios, e.g. in site-to-site tunnel mode, IPsec failover will only happen in one of end points.

19. Bandwidth control does not work when users select pre-defined services, e.g. http or "ftp.

20. Specific Service support for inbound traffic management is not work.

| 1.08B88_WW | 1. After delete IPsec one-to-one mapping rule, it could not drop the IPsec |

tunnel from DSR Web GUI.

2. After delete the IPsec one-to-one mapping rule, local PC is still able to ping remote PC with mapping IP address.

3. While changing the local network in IPsec policy, web GUI will display incorrect message.

4. The CLI: *security firewall ipv6 configure/edit* doesn't work.

5. There is an issue where the router is not able to transfer files > 250MB from Windows XP to USB storage after apply WinXP.reg script file.

6. Voice at LAN side client is not heard when the SIP Proxy resides in LAN.

7. Daylight saving with manual settings is not working properly for Newfoundland and Greenland time zones.

8. It's able to configure the same MAC address to WAN1 and WAN2 ports by selecting the 'Clone your PC's MAC Address' option.

9. After editing the WEP profile (wep-64), another WEP profile (wep-128) wireless client is not reconnecting until disable/enable the corresponding SSID.

10. Blank field for "data to supply to CA" when click view button in Self certificates requests page.

11. VLAN dropped in and dropped out packet entries are incorrect in dashboard page.

12. User cannot enable UPnP on LAN and VLAN simultaneously.

13. Bandwidth rules over IPsec VPN tunnel are not being followed.

14. Device keeps sending syslogs to syslog server after removing the earlier configured syslog server IP address.

15. USB storage is not working perfectly with windows XP. It's not able to open files without copying them locally and it has issue to copy larger files from Network Storage share on to the Windows XP host.

(Note: 1. Copy files from Windows XP to Network Storage works fine. 2. This issue doesn't affect Windows Vista, Windows 7 and Linux based operating systems)

16. IPSEC tunnel is not getting established after importing the exported file at the remote device until disable then enabling policy

17. Snmpwalk takes long time to display IPsec details.

18. Spillover threshold can't approach configured value very precisely.

19. IPsec failover only works for specific scenarios, e.g. in site-to-site tunnel mode, IPsec failover will only happen in one of end points.

20. Only first 25 PPTP/L2TP users in the user database can establish PPTP/L2TP tunnels.

	21. When device is configured using spillover mode and WAN2 is utilizing PPPoE to Internet, WAN2 will keep inactive, i.e. no responses to any requests from Internet, until spillover threshold value is touched. 22. Bandwidth control does not work when users select pre-defined services, e.g. http or "ftp.

1.08B77_WW	1. DSR routers don't support IPv6 Firewall and VPN current. Following CLI still doesn't work at all.
	
	    security firewall ipv6 default_outbound_policy
	    security firewall ipv6 configure/edit
	    security firewall ipv6 delete <row_id>
	    security firewall ipv6 disable <row_id>
	    security firewall ipv6 enable <row_id>
	
	2. There is an issue where the router is not able to transfer files > 250MB from Windows XP to USB storage after apply WinXP.reg script file.
	3. Voice at LAN side client is not heard when the SIP Proxy resides in LAN.
	4. Daylight saving with manual settings is not working properly for Newfoundland and Greenland time zones.
	5. It's able to configure the same MAC address to WAN1 and WAN2 ports by selecting the 'Clone your PC's MAC Address' option.
	6. After editing the WEP profile (wep-64), another WEP profile (wep-128) wireless client is not reconnecting until disable/enable the corresponding SSID.
	7. Blank field for "data to supply to CA" when click view button in Self certificates requests page.
	8. VLAN dropped in and dropped out packet entries are incorrect in dashboard page.
	9. User cannot enable UPnP on LAN and VLAN simultaneously.
	10. Bandwidth rules over IPsec VPN tunnel are not being followed.
	11. Device keeps sending syslogs to syslog server after removing the earlier configured syslog server IP address.
	12. USB storage is not working perfectly with windows XP. It's not able to open files without copying them locally and it has issue to copy larger files from Network Storage share on to the Windows XP host.
	  (Note: 1. Copy files from Windows XP to Network Storage works fine. 2. This issue doesn't affect Windows Vista, Windows 7 and Linux based operating systems)
	13. IPSEC tunnel is not getting established after importing the exported file at the remote device until disable then enabling policy

	14. Snmpwalk takes long time to display IPsec details.
	15. Spillover threshold can't approach configured value very precisely.
	16. IPsec failover only works for specific scenarios, e.g. in site-to-site tunnel mode, IPsec failover will only happen in one of end points.
	17. Only first 25 PPTP/L2TP users in the user database can establish PPTP/L2TP tunnels.
	18. When device is configured using spillover mode and WAN2 is utilizing PPPoE to Internet, WAN2 will keep inactive, i.e. no responses to any requests from Internet, until spillover threshold value is touched.
	19. Bandwidth control does not work when users select pre-defined services, e.g. http or "ftp.
1.08B51_WW	1. DSR routers don't support IPv6 Firewall and VPN current. Following CLI still doesn't work at all. *security firewall ipv6 default_outbound_policy* *security firewall ipv6 configure/edit* *security firewall ipv6 delete <row_id>* *security firewall ipv6 disable <row_id>* *security firewall ipv6 enable <row_id>* 2. There is an issue where the router is not able to transfer files > 250MB from Windows XP to USB storage after apply WinXP.reg script file. 3. Voice at LAN side client is not heard when the SIP Proxy resides in LAN. 4. Daylight saving with manual settings is not working properly for Newfoundland and Greenland time zones. 5. It's able to configure the same MAC address to WAN1 and WAN2 ports by selecting the 'Clone your PC's MAC Address' option. 6. After editing the WEP profile (wep-64), another WEP profile (wep-128) wireless client is not reconnecting until disable/enable the corresponding SSID. 7. Blank field for "data to supply to CA" when click view button in Self certificates requests page. 8. VLAN dropped in and dropped out packet entries are incorrect in dashboard page. 9. User cannot enable UPnP on LAN and VLAN simultaneously. 10. Bandwidth rules over IPsec VPN tunnel are not being followed. 11. Device keeps sending syslogs to syslog server after removing the earlier configured syslog server IP address. 12. USB storage is not working perfectly with windows XP. It's not able to open files without copying them locally and it has issue to copy larger files from

	Network Storage share on to the Windows XP host.
	(Note: 1. Copy files from Windows XP to Network Storage works fine. 2. This issue doesn't affect Windows Vista, Windows 7 and Linux based operating systems)
	13. IPSEC tunnel is not getting established after importing the exported file at the remote device until disable then enabling policy
	14. Snmpwalk takes long time to display IPsec details.
	15. Spillover threshold can't approach configured value very precisely.
	16. IPsec failover only works for specific scenarios, e.g. in site-to-site tunnel mode, IPSec failover will only happen in one of end points.
	17. Only first 25 PPTP/L2TP users in the user database can establish PPTP/L2TP tunnels.
	18. When device is configured using spillover mode and WAN2 is utilizing PPPoE to Internet, WAN2 will keep inactive, i.e. no responses to any requests from Internet, until spillover threshold value is touched.
	19. Bandwidth control does not work when users select pre-defined services, e.g. http or "ftp.

Related Documentation:

- Unified Services Router User Manual v2.02
- Unified Services Router CLI Reference Guide v2.00