Release Notes for DrayTek Vigor 2832 (UK/Ireland)

Firmware Version	3.9.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	14th November 2019
Build Date	17th October 2019
Applicable Models	Vigor2832, Vigor2832n
Revision	85525
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

(None)

Improvements

1. Improved SSL VPN compatibility with Apple devices. Self-Signed certificate's Valid To date is now 2 years from date of generation. Regenerate the router's Self-Signed Certificate to meet the new trusted certificate requirements of Apple iOS 13 & macOS 10.15. Longer Valid To periods can be specified by generating a Local Certificate and self-signing it with the router's internal Root CA.
2. Reporting Configuration added to [Management] > [TR-069] section where CPE Notification Settings log is disabled by default
3. [Diagnostics] > [Traffic Graph] improved
4. The router would stop responding when the SSH session from a LAN PC times out
5. In some scenarios, it was not possible to resume watching IPTV services through the router after pausing the IPTV video service for 5 minutes or more
6. Router instead of local AP replied to SNMP requests
7. OpenVPN port 1194 can be redirected/open
8. The Policy Route profiles configured with different NATed VPN interfaces could not work when more than one NATed VPN tunnel was established
9. IPsec Xauth VPN connection could not be established in some circumstances
10. Unable to show correct DNS server IP address set for different LANs on [System Status] page
11. Restricted administrator from adding scripting in the Web portal message
12. SSL VPN tunnel could remain offline in some scenarios
13. Local GRE Server could not receive GRE packets from Internet even when configured as a DMZ host
14. Improvements to IGMP proxy and fast leave in multi-subnet environment
15. Unable to display correct WAN IP address for DDNS Log when using Internet IP

Known Issues

1. **Important Note** – PPTP VPN services are now disabled by default.
   This only affects the factory default configuration, which is loaded upon pressing the router's Factory Reset button, or reflashing with .rst firmware. Upgrading the firmware with .all file will not impact VPN settings.

Firmware File Types

The ZIP file contains the firmware with two different file extensions, .ALL and .RST. The firmware is identical but the RST file contains factory default settings. If you install the ALL file, your router will retain all existing settings. If you use the RST file, <u>all settings will be wiped from your router</u>.

Upgrade Instructions

It is recommended that you take a configuration backup prior to upgrading the firmware. This can be done from the router's system maintenance menu.

To upgrade firmware, select *'firmware upgrade'* from the router's system maintenance menu and select the correct file. Ensure that you select the ALL file <u>unless</u> you want to wipe out your router's settings back to factory default.

Manual Upgrade

 If you cannot access the router's menu, you can put the router into 'TFTP' mode by holding the RESET whilst turning the unit on and then use the Firmware Utility. That will enable TFTP mode. TFTP mode is indicated by all LEDs flashing. This mode will also be automatically enabled by the router if there is a firmware/settings abnormality. Upgrading from the web interface is easier and recommended – this manual mode is only needed if the web interface is inaccessible.

Firmware Version	3.9.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	16th July 2019
Build Date	5th June 2019
Applicable Models	Vigor2832, Vigor2832n
Revision	82550
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

1. Service activation status can now be verified from [MyVigor Services] > [Service Status]

Improvements

1. Text for the license expired page modified
2. Improved display of NAT Open Port and Port Redirection rules
3. Improved mechanism for disk usage and storage management on USB drive
4. Additional help links added to the router's GUI
5. The QoS Class Rule Setup process simplified
6. Customised DDNS profile can accept an IP address for the Provider Host
7. DHCP option 121 will update the routing table
8. Disabling HTTP service would trigger a Port Conflict message
9. A new 58DDNS DDNS provided added in [Applications] > [Dynamic DNS]
10. Serial number will synch with VigorACS
11. IPsec EAP option added to IKEv2 LAN to LAN VPN to use X.509 for authentication
12. Restoring configuration with a password did not display a pop-up window to enter a password.
13. Remote Dial-in username did not accept "\" and "\u" characters
14. Improved QoS Class Ration compatibility with VigorACS
15. [VPN and Remote Access] > [LAN to LAN] profile Mode set to Routing
16. IPv6 IP address did not display correctly on the dashboard after rebooting the router
17. XAuth VPN profile setup improved
18. Unable to add more than 12 IP addresses for virtual IP mapping (IPsec LAN to LAN VPN profile)
19. OpenVPN clients could be unable to establish a VPN tunnel under some conditions
20. Improvements to LAN-to-LAN mechanism for scenarios with more than 20 VPN tunnels
21. OpenDNS DDNS update mechanism improved
22. WDS Bridge did not work with VigorAP902 when PSK for WDS and SSID were independent
23. Smart VPN Client download links led to the wrong pages
24. An error message appeared when SSH client tried to exit the SSH connection
25. A new telnet command added to set TCP RST packet timeout
26. Telnet command 'ipf flowtrack set -e' did not work
27. Telnet command "vpn pass2nat off" adds support for 'Pass Routing LAN to VPN'
28. IKEv2 default encryption was set to DES without authentication
29. Unable to set and save IPsec IKEv2 setting on LAN to LAN successfully

30. Hotspot web portal did not work with Facebook
31. The "server response" field added to custom SMS Service Object
32. TR-069 parameter for WAN1 >> PPPoE >> Fallback account added
33. DHCPv6 with Prefix Delegation for WAN added
34. Brute Force mechanism improvements
35. Any IP could be used for hardware acceleration even if it was not specified as the specific host
36. "Pre-Shared Key cannot be empty" notification added for the IPSec VPN profile page
37. QoS status for each WAN/Class and VoIP status information added
38. Improved VigorACS registration mechanism
39. Incorrect port status was shown in the ARP table when a wireless device connected to WDS
40. Remote dial-in (IKEv2 X.509) users could not establish VPN with the router
41. Policy routes with different NATed VPN interfaces would not work when more than one NATed VPN tunnel was established
42. TR-069 parameter to execute the telnet command by VigorACS server added
43. OpenVPN clients could be unable to establish a VPN tunnel under some conditions
44. APPE service mechanism improved
45. Wireless 802.1x clients were unable to obtain an IP address from relayed DHCP server
46. IGMP fast leave mechanism improved
47. USB Printer Server disabled by default
48. DrayDDNS profile was disabled in some circumstances
49. It was not possible to switch to NAT mode when setting up LAN to LAN Dial-Out profile with IKEv2 EAP
50. The HOST ID field displayed interface name in [LAN] > [Bind IP to MAC] ARP Table section

Known Issues

(None)

Firmware Version	3.9.0 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	5th March 2019
Build Date	18th February 2019
Applicable Models	Vigor2832, Vigor2832n
Revision	79929
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

1. OpenVPN is now supported as a Remote Dial-in User VPN protocol.

   Important Note: The router's OpenVPN server is automatically enabled on the router upon upgrade to 3.9.0 firmware, which listens on TCP & UDP ports 1194 by default and will take precedence over port forwarding to a LAN server using these ports.
   This service and its listening ports can be configured from the [VPN and Remote Access] > [OpenVPN] menu, or disabled in [VPN and Remote Access] > [Remote Access Control]

2. Bypass Load Balancing for specified traffic types in [WAN] > [General Setup] > [Advanced]
3. Search box added to main menu to search for sub menus
4. IKEv2 EAP is now supported as a Remote Dial-in User VPN protocol
5. Added Brute Force Protection for router management interfaces to [System Maintenance] > [Management]

Improvements

1. New WAN Connection Detection mode for Ethernet / MPoA WAN – "Strict ARP Detect"
2. Improved page layout in [USB Application] > [Modem Support List]
3. Improved Quality of Service Class Rule list layout – Single list for Rules in Class 1,2 & 3
4. Improved PPPoE ISP interoperability by adding support for configurable PPP LCP Echo Request options
5. Specify Remote Client IP option did not work for PPTP on VPN
6. After disabling the option of Allow management from the Internet, WAN IPv6 blocked the web access via HTTP/HTTPS when both port numbers for SSL VPN and HTTPS were set as 443
7. Configuration files for LAN to LAN VPN, Bind IP to MAC and Wireless ACL could not be restored if IPv6 was disabled on the router
8. Data Flow Monitor did not display RX traffic when downloading through VPN tunnel
9. An error message was displayed when clicking Check the Latest Firmware button in [System Maintenance] > [Firmware Upgrade]
10. Resolved an issue with configuring [LAN] > [LAN Port Mirror] settings
11. iPad / iPhone devices with iOS 10.3.1 and later could not establish IKEv2 VPN tunnel
12. LAN VLAN Tags were not correctly handled with IPv4 Fragmented Packets
13. Enabling User Management could affect NAT Loopback
14. Improved interoperability of IKEv2 IPsec VPN Tunnel with Google Cloud VPN service

15. Data Quota configured in [User Management] > [User Profile] could be reset to zero after re-login
16. Specify Remote Client IP option did not work for PPTP Remote Dial-In User VPN connections
17. Support Anti-Spoofing function
18. Support IPTV diagnosis

Known Issues

1. See New Features entry #1 for notes on OpenVPNs impact on Port Redirections for TCP/UDP port 1194
2. VPN Menu options for IKEv2 and XAuth can be selected in [LAN to LAN] – Dial-Out IPsec Tunnel but cannot currently be configured. This will be resolved in the next firmware release

Firmware Version	3.8.9.3 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	10th September 2018
Build Date	17th August 2018
Applicable Models	Vigor2832, Vigor2832n
Revision	75974
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

1. SNMP monitoring clients can now read out the CPU load and memory usage percentages as part of the router and firmware details in the sysDescr.0 (OID 1.3.6.1.2.1.1.1) value

Improvements

1. Disabling a port redirection from the summary view ([NAT] > [Port Redirection]) rather than the profile entry itself did not disable the port forwarding entry
2. NAT loopback could not operate with port forwards configured using ports 768 to 1023

Known Issues

(None)

Firmware Version	3.8.9.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	16th August
Build Date	27th July 2018
Applicable Models	Vigor2832, Vigor2832n
Revision	75582
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

(None)

Improvements

1. Quality of Service did not display WAN1's ADSL sync speeds in f/w 3.8.9 & 3.8.9.1
2. Improved interoperability with Hotspot Web Portal and Facebook authentication service
3. USB Thermometer was not detected in some configurations
4. Web interface could not be accessed via HTTPS from some network environments

Known Issues

(None)

Firmware Version	3.8.9.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	21st June 2018
Build Date	12th June 2018
Applicable Models	Vigor2832, Vigor2832n
Revision	74521
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

Security Advisory

1. Check your DNS and DHCP settings on your router.
   https://www.draytek.co.uk/support/security-advisories/kb-advisory-csrf-and-dns-dhcp-web-attacks
   If you have a router supporting multiple LAN subnets, check settings for each subnet. Your DNS settings should be either blank, set to the correct DNS server addresses from your ISP or DNS server addresses of a server which you have deliberately set (e.g. Google 8.8.8.8). A known rogue DNS server is 38.134.121.95 - if you see that, your router has been changed.

New Features

1. Firewall Filter rules can now be linked to specified LAN and WAN interfaces by selecting a Direction then clicking Advanced and selecting the interfaces that the Filter rule will affect
2. Support DrayOS IKEv1 IPsec XAuth as a VPN protocol for Remote Dial-In User VPN tunnels
3. Support for EAP Tunnelled Transport Layer Security (EAP_TTLS) security method added to [Applications] > [Local 802.1X General Setup]
4. Configuration backup / restore is now available for Remote Dial-In User and LAN-to-LAN
5. Larger certificate files now supported in [Certificate Management] > [Local Certificate] making it possible to include additional certificates required to complete a certificate chain
6. Wireless Pre-Shared Key can now be viewed when logged into the router's admin account. Click on the "****" text to reveal the password currently in use
7. LAN ports, Wireless LAN button and Factory Reset button can now be enabled or disabled from [System Maintenance] > [Panel Control]

Improvements

1. Fixed the App Enforcement profile issue in 3.8.9 firmware
2. Fixed the Web UI Issue if Bandwidth Limit and Data Flow Monitor were enabled in 3.8.9 firmware
3. Factory Default configuration now enables WAN2 port instead of operating as LAN5 port
4. Support for VigorACS 2 version 2.3.0
5. Layout of [WAN] > [Internet Access] > [Details Page] improved to group essential settings in the left pane, with additional / advanced options grouped in the right pane
6. Subnet Mask settings in the web interface now use a drop-down box for selection
7. The number of characters allowed in a text box, such as a username or password field, is now displayed in the web interface when no text is entered in that text box
8. Layout of [VPN and Remote Access] > [Connection Management] improved with separate tabs for active LAN-to-LAN and Remote Dial-In User VPN tunnels

9. Layout of [Bandwidth Management] > [Quality of Service] improved, WAN1 Bandwidth is now configured manually
10. Schedule entries are now selected from a drop-down box which displays each schedule entry number and configured Comment fields
11. DoS Defence moved to [Firewall] > [Defence Setup]
12. Anti-Spoofing Defence settings for IP and ARP spoofing added to [Firewall] > [Defence Setup]
13. Certificate import can now be performed via CLI using "mngt cert_import" command via URL
14. Removed deprecated CLI commands "ip dmz" and "ip aux [Join to NAT pool]"
15. Added "IPv6 Address Random Allocation" option for DHCPv6 Server settings
16. IKEv2 LAN to LAN VPN tunnels can specify these new Proposal options:
    a. Diffie-Hellman (DH) Group 19 (256-bit Elliptic Curve)
    b. Diffie-Hellman (DH) Group 20 (384-bit Elliptic Curve)
    c. Diffie-Hellman (DH) Group 21 (512-bit Elliptic Curve)
17. When upgrading firmware, selecting a firmware file and clicking the "Preview" button will display details of the firmware selected
18. Improved load balancing algorithm for VoIP – STUN and SIP connections will now remain on the same WAN interface by default
19. Session timeout values for SSH and Telnet can now be adjusted with "mngt telnettimeout/sshtimeout" CLI commands
20. Improved interoperability of the DHCP Relay function with Windows Server's DHCP server
21. DHCP Relay did not work with Remote Dial-In User VPN tunnels
22. The Domain Name "ddns.net" could not be selected when using No-IP.com Dynamic DNS
23. Added support for EntryDDNS Dynamic DNS provider
24. Multiple objects can now be selected configuring an object group
25. Added "Next" and "Previous" links on each object profile editing page
26. DHCP Broadcast packets from LAN clients could incorrectly be sent out through the WAN2 interface in some circumstances, affecting WAN2 connections using DHCP for IP allocation
27. Auto VoIP QoS is now applied to routed LAN subnets and VPN tunnels
28. Restart is no longer required for changes to [Applications] > [RADIUS/TACACS+] > [Internal Server] when enabling/disabling Internal Radius Server or modifying the Authentication List
29. Added switching between viewing All Users and Online Users view in [User Management] > [User Online Status] by clicking on the text in the upper right
30. Bind IP to MAC was incorrectly limited to 300 entries instead of 1024
31. Increased Hotspot Web Portal profile Terms and Conditions Content field length to 1360 characters
32. Added "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" cipher for SSL VPN
33. Added IGMP v3 Source-list support
34. Support WAN DHCP option 121 for adding new static route
35. Resolved display issue in [NAT] > [Port Redirection] when configuring Service Name
36. With LAN1 and LAN2 subnets enabled and LAN3 / LAN4 subnets disabled, the [LAN] > [General Setup] page could incorrectly show that LAN3 / LAN4 were enabled
37. RIPng protocol could not be enabled for LAN2's [IPv6] > [Advanced Setting]
38. Valid configuration settings for LAN2's [IPv6] > [Advanced Setting] Router Advertisement Configuration could not be saved due to a validation error

Firmware Version	3.8.9 (Not Released)
Release Date	-
Build Date	28th May 2018
Applicable Models	Vigor2832, Vigor2832n
Revision	74161
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

Security Advisory

1. Check your DNS and DHCP settings on your router.
   https://www.draytek.co.uk/support/security-advisories/kb-advisory-csrf-and-dns-dhcp-web-attacks
   If you have a router supporting multiple LAN subnets, check settings for each subnet. Your DNS settings should be either blank, set to the correct DNS server addresses from your ISP or DNS server addresses of a server which you have deliberately set (e.g. Google 8.8.8.8). A known rogue DNS server is 38.134.121.95 - if you see that, your router has been changed.

New Features

(See Firmware 3.8.9.1)

Improvements

(See Firmware 3.8.9.1)

Known Issues

1. The router cannot be managed from the Web UI if Bandwidth Limit is enabled on the router. This will be corrected in the next firmware release.

Firmware Version	3.8.8.2
Release Type	**Critical** – Upgrade recommended immediately
Release Date	18th May 2018
Build Date	18th May 2018
Applicable Models	Vigor2832, Vigor2832n
Revision	73962
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

None

Improvements

1. This firmware includes improvements to harden the web interface against attacks. We have become aware of specific attacks against router, including DrayTek models where hackers have altered specific settings relating to your DNS servers and DHCP settings. You should urgently check those settings on your router. If they appear to have been tampered with, correct them and change your admin password and for any other config anomalies. Restore a config backup if you have one (from prior to the attack). We continue to investigate this issue but the first priority was to issue updated firmware

Known Issues

(None)

Firmware Version	3.8.8
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	12th February 2018
Build Date	19th January 2018
Applicable Models	Vigor2832, Vigor2832n
Revision	71280
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

(None)

Improvement

1. Improvements to [CSM] > [Web Content Filter Profile] / [URL Content Filter Profile] > [App Enforcement Profile] / [DNS Filter] menus
2. Firmware could only be upgraded through Firmware Upgrade Utility 3.6.6 when router was manually put into TFTP mode
3. Resolved an issue that could cause Bind IP to MAC to operate incorrectly in some configurations

Known Issues

(None)

Firmware Version	3.8.7
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	3rd January 2018
Build Date	1st December 2017
Applicable Models	Vigor2832, Vigor2832n
Revision	70316
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

1. Supported LAN subnet size increased to 1023 IP addresses per subnet (/22)
2. Support for IPsec IKEv2 for LAN to LAN tunnels and Remote Dial-in User VPN clients that support Pre-Shared-Key authentication
3. EAPOL Key Retry Enable/Disable setting added to [Wireless LAN (2.4GHz/5GHz)] > [Security] Disabling this setting can prevent WPA2 Key Reinstallation Attack (KRACK) attack vectors, for more details please read this security advisory: https://www.draytek.co.uk/information/our-technology/wpa2-krack-vulnerability (EAPOL Key Retry is set to Enabled by default and in previous firmware)
4. LAN Access Control can now disable management interface(s) for LAN1
5. Firewall configuration can be backed up / restored from [Firewall] > [General Setup]
6. WAN Failover in [WAN] > [General Setup] now supports Failover by Traffic Threshold

Improvement

1. When a wireless client attempts to authenticate with the router's wireless network, syslog will now send messages for WPA2's 4-way handshake, to allow for troubleshooting of the new "EAPOL Key Retries" setting
2. IPv6 WAN interface connection detection mode now defaults to "Always On"
3. Improvements to the interface of the [Applications] > [Local 802.1X General Setup] page
4. Changing the router's HTTP or HTTPS management ports could stop the DNS Filter block message from being displayed
5. Improved LDAP server interoperability when authenticating L2TP with IPsec connections
6. Port forwarding through [NAT] > [Open Ports] could stop working with some network configurations
7. DDNS Syslog information could report WAN status incorrectly
8. PPTP VPN connections could not be successfully authenticated with TACACS+
9. Enabling Session Limit could stop NAT port forwarding (Open Ports / Port Redirection / DMZ) from operating correctly

Known Issues

(None)

Firmware Version	3.8.3.5
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	10th August 2017
Build Date	18th July 2017
Applicable Models	Vigor2832, Vigor2832n
Revision	67044
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

1. Support for extra TR-069 parameters
2. Router auto-generates unique Self-Signed Certificate for HTTPS [System Maintenance] > [Self-Signed Certificate]

Improvement

1. TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher disabled for SSL VPN & HTTPS management
2. LAN clients can no longer access the router management interface(s) outside of their own VLAN
3. Route Policies could not apply in NAT mode to Static & Dynamic IP mode WAN interface(s)
4. Improved Content Filtering of Youtube when accessed through the Google Chrome browser
5. Resolved an issue with NAT loopback when forwarding to WAN IP Alias addresses
6. Improved SIP ALG functionality with NAT loopback
7. [Diagnostics] > [Ping Diagnosis] displayed output incorrectly when pinging through a VPN tunnel
8. [Hotspot Web Portal] could not redirect to specified URL when using SMS login method
9. LAN DNS is no longer case sensitive
10. When SSL VPN service port was disabled, TCP 443 could be detected on WAN side (but no access permitted)
11. Route Policy Diagnostics would indicate an incorrect rule for Route Policies with a domain name specified as the destination

Known Issues

(None)

Firmware Version	3.8.3.4
Release Type	**Regular** – Upgrade recommended when convenient Note: The previous firmware (3.8.3.3) was a **critical release**. This f/w includes all changes/improvements that were in 3.8.3.3.
Release Date	13th April 2017
Build Date	22nd March 2017
Applicable Models	Vigor2832, Vigor2832n
Revision	63523
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

1. [Hotspot Web Portal] replaces [LAN] > [Web Portal Setup]
2. Support for [Wireless LAN] > [Airtime Fairness] added
3. Central AP Management over VPN support added, manage VigorAPs connected to a remote Vigor 2832 series router from a Vigor router that supports Central AP Management
4. SIP ALG can be configured in the web interface from [NAT] > [ALG]

Improvement

1. PPTP VPN's Dial-In PPP Authentication can now limit connections to "MS-CHAPv2 Only"
2. NAT Loopback did not work when connecting to Routed LAN interfaces
3. 2.4GHz wireless driver updated
4. Improvements to NAT & Routing throughput performance
5. WAN Budget could not send alerts for WAN interfaces with Hardware Acceleration enabled
6. Resolved an issue with DNS SEC that affected DNS resolution for Dial-In VPN clients
7. The router did not process RIP packets correctly for interfaces with RIP enabled
8. Resolved an issue with VLAN tags in some network configurations

Known Issues

(None)

Firmware Version	3.8.3.3
Release Type	**Critical** – Upgrade recommended immediately
Release Date	20th December 2016
Build Date	6th December 2016
Applicable Models	Vigor2832, Vigor2832n
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features in this Firmware

(None)

Improvements in this firmware

1. Security improvements including one or more considered critical.
2. Misc. minor WUI changes/corrections.

Known Issues

(None)

Firmware Version	3.8.3.2
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	10th October 2016
Build Date	23rd September 2016
Applicable Models	Vigor2832, Vigor2832n
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

New Features

1. Support for [Hardware Acceleration] of WAN2
2. Support for new firmware availability notification
3. Device name is now displayed in notification emails sent by the router
4. Improved HW acceleration functionality to allow Hardware Accelerated data to display in WAN Budget, Traffic Graph, Data Flow Monitor and Online Status
5. The router's Online Status can display "Remote DSL" information from a Vigor 130 or Vigor 120v2 modem connected to the router's WAN ports
6. Added [NAT] > [ALG] menu to configure the router's SIP ALG (Application Layer Gateway) functionality
7. [Applications] > [Schedule] re-designed to simplify management of schedules

Improvements

1. Added an option to change TTL value for WAN2 to improve compatibility with some ISPs
2. Support for configuring TR-069 URL via DHCP option 43 added to [System Maintenance] > [TR-069]
3. TR-069 parameters added to allow configuring [NAT] > [DMZ Host] WAN Alias IPs through VigorACS
4. Added options in [System Maintenance] > [Management] to disable HTTPS management via TLS 1.0, TLS 1.1 or TLS 1.2
5. Improvements to [WAN] > [WAN Budget] web interface
6. Improved interoperability of Ethernet WAN2 interface
7. [VoIP models] Additional WAN registration options added for SIP accounts
8. Resolved an issue that could stop Bandwidth Limit from working if the Firewall was disabled
9. QoS bandwidth mechanism improved for low bandwidth values

Known Issues

(None)

Firmware Version	3.8.3.1
Release Date	13th June 2016
Build Date	1st March 2016
Applicable Models	Vigor2832, Vigor2832n
ADSL Modem Code	661701
Locale	UK Only / Annex A Only

First Firmware Release for this model

Known Issues

(None)

[END OF FILE]