NO:AP1101-2 V.1

Release Note for Vigor3220 Series

Firmware Version:	3.9.1
Release Type:	Normal
Applied Models:	Vigor3220/Vigor3220n

Vigor3220 Series, a broadband router, integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) for VPN tunnels.

New Features

- Support IPTV diagnosis.

Improvement

- Improved: Add the MyVigor Services>>Service Status page to display the service activation information.
- Improved: Add the Station Control field in Central Management>>AP>>WLAN Profile.
- Improved: Support Exception list for load balance in WAN>>General Setup.
- Improved: For telnet command setting, give full parameter names for getting/setting all TR-069 parameters.
- Improved: Add a note to notify the user that the Vigor router certificate is not part of the configuration file.
- Improved: Add a check box to hide Group Password in Central Management >> Switch >> Profile page.
- Improved: Support the IP Group as Source IP on Port Redirection/Open Ports.
- Improved: Add a TR-069 parameter of VoIP QoS for configured by VigorACS.
- Improved: Add search bar to Left Menu.
- Improved: Remove the TFTP note from System Maintenance >> Firmware Upgrade.
- Improved: Add the Dynu DDNS provider as a Provider Host selection.
- Improved: Support IKEv2 EAP LAN to LAN tunnel for using with NordVPN server.
- Improved: Improve the timing of sending the RMM information.
- Improved: Support "Use ACS Server" as the STUN server on System Maintenance>>TR-069 Setting.
- Improved: The USB printer server is disabled in default.

- Corrected: Unable to upgrade/downgrade firmware version on System Maintenance >> Firmware Upgrade.
- Corrected: Vigor router rebooted when OpenVPN client was connecting.
- Corrected: Vigor router started to reboot every two minutes after twenty-one VPN tunnels were on.
- Corrected: Failed to connect to the remote client by "SSL LAN to LAN".
- Corrected: Open Port setting (for accessing to the device behind the dialing out router) was invalid if LAN to LAN VPN profile 1 was not used.
- Corrected: Abnormal status displayed on the Central Management>>External Device page (switch connect to tagged VLAN).
- Corrected: Failed to send Auth code via custom SMS for 2-Step Authentication web login.
- Corrected: Unable to use port 1194 for TCP/UDP even OpenVPN service was disabled.
- Corrected: Unable to obtain QoS Class Ratio setting from VigorACS server.
- Corrected: The wireless 802.1x clients were unable to obtain an IP address from the relayed DHCP server.
- Corrected: Unable to register to VigorACS.
- Corrected: Failed to create IKEv2 EAP connection from Windows 10 when using self-signed CA.
- Corrected: Unable to restore VPN backup profile from other router to Vigor3220.
- Corrected: Android or Windows10 OS built-in detection page still popped up even if Captive Portal Detection was disabled for the web portal setup.
- Corrected: Unable to accept VPN remote dial-in users when "change default route to this VPN tunnel" was enabled for the LAN to LAN.
- Corrected: Unable to authenticate VigorACS server certificate (issued by Let's Encrypt).
- Corrected: Unable to resume IPTV after pausing for more than 5 minutes.
- Corrected: SSL VPN client obtained DNS server address via router's WAN instead of DHCP Relay server.

Known Issue

- None.

Note

- Use MFUU Tools or Console TFTP to upgrade firmware version if failing to use web user interface for firmware upgrade.

RD NO: 108_06_27