

Release Note for Vigor2133 Series

Firmware Version:	3.9.4.1
Release Type:	Normal
Applied Models:	Vigor2133/Vigor2133n/Vigor2133ac/Vigor2133Vac/Vigor2133FVac

Vigor2133 features advanced bandwidth control mechanism such as IP-layer, QoS, NAT Session Limitation, Bandwidth Borrowed, etc., to allow easy, flexible, reliable access control and bandwidth management.

New Features

- None.

Improvement

- Improved: Support WAN IP alias for Dynamic DNS.
- Improved: Allow the router remote management over L2TP WAN.
- Improved: Support the IP group selection in WAN management ACL.
- Improved: Add the option of MS-CHAPv2 for WAN PPP Authentication.
- Improved: Modifications of the options for Monthly Cycle Day on WAN >> WAN Budget.
- Improved: Check the policy route rule at the same time, while doing the source subnet checking for NAT.
- Improved: Adjust router's self-signed certificate to comply with new browser restrictions. Start on 2020-09-01, many client Oses/browsers will enforce publicly trusted TLS server certificate lifetime to 398 days or less, and connections will be rejected if the certificates violated this rule, so this firmware patch will automatically re-sign all the self-signed certificates lifetime to 395 days (was 2 years or longer in older versions).
- Corrected: An issue of voice quality.
- Corrected: A display issue of APPE WUI.
- Corrected: An issue of port number 5060 not working for NAT.
- Corrected: An issue of quotation marks used for password setting.
- Corrected: An issue of source IP in Open Ports blocked other Open Ports entries.
- Corrected: An issue of Isolate LAN setting of WLAN profile for AP management.
- Corrected: An issue of display error for the Comment on Wireless LAN >> Access Control.
- Corrected: An issue of incoming VoIP calls blocked by the firewall default rule (block) even if the actual filter rule set with "pass".

TR-069

- Improved: Allow TR-069 traffic pass though VPN tunnels in NAT mode.
- Corrected: An issue of failure to respond LAN host info through TR-069.
- Corrected: An issue of failing to connect VigorACS when ACS Server On set with LAN1/VPN on TR-069 Setting page.

VPN

- Corrected: An issue of Let's Encrypt certificate generation.
- Corrected: An issue of RIP protocol not working (LAN to LAN).
- Corrected: A stability issue of SSL "LAN to LAN" VPN connection.
- Corrected: An issue of failure to dial-out a specific LAN to LAN tunnel.
- Corrected: An issue of IP address assignment of OpenVPN server to the OpenVPN client.
- Corrected: An issue of failing to forward NetBios naming packet & multicast packets via OpenVPN.
- Corrected: Corrected: An issue that IKEv2 EAP Client by Static IP assignment failed to access VPN network after Rekey.
- Corrected: An issue that the username was not displayed on VPN Connection Status after dialing Host to LAN (OpenVPN) via RADIUS server authentication.

Known Issue

- None.