NO:AP1101-2 V.1

Release Note for Vigor1000B

Firmware Version:	4.3.2
Release Type:	Normal
Applied Models:	Vigor1000B

New Features

- Support multilingual login page.
- Support Smart Action via telnet command.
- Support 2 FA authentication for VPN connection.
- Manage VigorSwitch FX2120, PQ2200xb, Q2200x, P1282 and G1282 by SWM (switch management).

Improvement

- Improved: Support UDP Broadcast over VPN.
- Improved: Improve the WireGuard VPN feature.
  - stability
  - support "bind to WAN"
- Improved: The APPE module gets upgraded from 15.25 to 15.27.
  - Add the APPE, Statistic, and Route Policy functions related to Yahoo!
  - Add Zalo to the APP Enforcement.
- Improved: Support sending via WAN IP Alias for NTP and Mail Alert.
- Improved: MSS can be changed according to MTU (MSS = MTU-140) automatically.
- Improved: Increase the length of characters for username and password fields in Mail Service Object from 32 to 128.
- Improved: Extend the validity of certificate generated by router for OpenVPN server/client from 1 year to 10 years.
- Corrected: An issue with the LAN DNS malfunction.
- Corrected: An issue with TR-069 exhausted sockets.
- Corrected: An issue of incomplete DrayDDNS logs.
- Corrected: An issue with the SFP LEDs not working.
- Corrected: An issue with memory leakage in WireGuard.
- Corrected: An issue with IKEV2 VPN users got disconnected during rekey.
- Corrected: An issue with the malfunction for DHCP relay with tagged VLAN.
- Corrected: An issue with the SSL VPN stability (some NULL pointer problems).
- Corrected: An issue where CPU usage was high and also VPN ping was high.

- Corrected: An issue of a slow Internet connection with SUMITOMO modem.
- Corrected: An issue of VPN clients got duplicated IP when DHCP relay enabled.
- Corrected: An issue of buffer leakage when SSL VPN dial-out failed in linking state.
- Corrected: Issues where several WUI did not show correctly after upgrading to 4.3.1.1.
- Corrected: An issue where an untagged PC got an IP from a network that had a VLAN tag.
- Corrected: An issue where SSL VPN stopped responding and router hung after some days.
- Corrected: An issue of router reboot after configuring "Load Balance Policy" for VPN Trunk.
- Corrected: An issue with the system rebooting continuously when WAN/LAN IPv6 was enabled.
- Corrected: An issue of switch management not working when using more than 16 LAN/VLANs.
- Corrected: An issue of virtual WAN traffic (from "the same as physical wan traffic" to the actual virtual wan traffic).
- Corrected: An issue in which SNMPv3 agent was unable to get data successfully when privacy algorithm was AES.
- Corrected: An issue where H2L clients could not access LAN after changing VPN protocols between PPTP and SSL.
- Corrected: An issue with some of the WANs in "WAN>> Multi-VLAN" was unable to establish the PPPoE connections.
- Corrected: An issue with intermittent packet loss when routing through load balance policy using IP alias on a HA setup.
- Improved: Revert the experimental FAST NAT feature to an older but more stable version (e.g. eliminated duplicate portmap).
- Improved: Revert multi-wan support for route policy back to an older but more stable version.

Known Issue

- The web portal may cause the router to be too busy to respond quickly.
- A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management, NAT loopback traffic, and VPN access. It is recommended to review the firewall settings before upgrading.
- When the firmware is downgrading via “System Maintenance >> Firmware Upgrade”, one might have a chance to experience a config compatibility error, which causes the config of a certain function to return to the default setting. To avoid this error, “System Maintenance >> Configuration Export >> Restore Firmware with config” is the preferred way for firmware “downgrading”. We suggest backup the config file before upgrading any firmware as well.