

RVL200 Firmware v1.1.7 Release Note

8/08/2007

If you are upgrading the firmware from v1.1.x to v1.1.7, you may find the status window turning into blank in the middle of firmware upgrade. Should that happen, please leave it alone for another 15 minutes and the upgrade will complete without problem. If the upgrade fails and the DIAG LED is blinking, a TFTP utility (available on linksys.com) can be used to push the firmware to the router.

Issues Fixed:

1. Fixed the PPPoE issue where connection will fail to establish when the PPPoE username contains a # sign.
2. Fixed the issue where the firewall status (SPI/DoS/BlockWANRequest/RemoteManagement) is not shown correctly in the System Summary page when the firewall is disabled.
3. The IP Range of Virtual Passage was changed to 6, instead of 10.
4. Removed the reference to Priority in the Help page of Port Management->Port Setup, since the setting is supposed to be configured on the QoS page.
5. Fixed the issue where the packet will appear coming from the router's LAN IP, when a packet is forwarded to the DMZ Host in the LAN of RVL200.
6. Fixed an issue with PPTP Passthrough.
7. Renamed "IGMP Proxy" as "Multicast Passthrough" on the Firewall->General page.
8. Added Policy Name to the Access Rule configuration page.
9. Time Zone description and index were modified.
10. Support self-generated SSL certificate and allow SSL certificates (in .PEM format) to be imported.
11. Virtual Passage supports Mac OS X 10.4.x (with Safari), Linux (with Firefox 2) and Windows 2000/XP/Vista (with Internet Explorer 6/7, Netscape Communicator 8, and Firefox 2.) Note that JRE is required for Virtual Passage on Linux. Also note that when a user wants to establish the SSL VPN from a Windows Vista for the first time, he needs to run the Internet Explorer as Administrator because the Virtual passage installation can only be done with the admin rights.
12. Virtual Passage supports Windows Workgroups. To resolve NetBIOS names over SSL VPN, the admin has to configure a WINS Server on the DHCP page of RVL200, and the remote user's PC has to configure its TCP/IP Property to point to this WINS Server.
13. Virtual Passage client can now run on Windows 2003 Server.
14. RADIUS client now supports CHAP, MSCHAP, MSCHAPV2 in addition to PAP for user authentication.
15. DHCP Server supports multiple subnets that correspond to multiple VLANs. Inter-VLAN routing is supported for the VLANs that are on different subnets.
16. DHCP Server supports static IP and MAC address binding.
17. Help page updated to show how to use the MAC Address Filtering feature.
18. Support One-to-One NAT.
19. Port Mirroring. Admin can specify one of the LAN ports as the target port, and select one or more ports to be mirrored. This feature can be configured on the System Management->Port Mirroring page.
20. Compliant with the UPnP IGD Certification.

21. Support more configurable options for logging in the Log->System Log page.
22. Tagged events with severity level. Logged events can be viewed/filtered according to the selected severity level.
23. Added Outgoing Log Table and Incoming Log Table into the System Log page.
24. Support SNMPv3.
25. Support SNMP Traps for LAN port Link-up and Link-down detection.

26. IPSec: NetBIOS Broadcast
27. IPSec: Remote Security Group Type supports IP Range
28. IPSec: Keying Mode supports Manual Mode
29. IPSec: Gateway-to-gateway tunnel supports IP payload compression.
30. IPSec: Phase2 Encryption & Authentication supports Null.

31. IPSec Passthrough supports multiple sessions.
32. PPTP Passthrough supports multiple sessions.
33. The SSH Sentinel VPN Client can establish an IPSec tunnel with RVL200 with the NAT Traversal enabled.
34. Access Rules and Content Filters support 24-hour format for scheduling.
35. Support Manual Daylight Saving, where the start and end dates can be manually specified.

36. Support SIP Application Layer Gateway, which can be enabled/disabled on the Firewall->General page.
37. Support IGMP Snooping.
38. Content Filters can be defined for groups of computers identified by IP or MAC addresses.
39. Email Alert supports password authentication, i.e. NTLM authentication on Microsoft Exchange Server.

Known Issues:

1. Mac OS version 10.4 is known to have a image loss issue with several https servers, including RVL200.
Images files transmitted over a SSL tunnel can be lost randomly. Mac OS version 10.4.8 has fixed this issue.
2. Syslog may stop working after the router has been up for a few days.
Rebooting the router can temporarily fix the problem.