Release Notes for Cisco RV Series Multi-WAN VPN Routers Firmware Version 4.0.2.08

May 2011

This firmware is the first maintenance release for hardware Version 3 of the RV Series Multi-WAN VPN Routers, including RV042, RV082 and RV016. Hardware Version 3 supports all the features of earlier versions of the RV Series Multi-WAN VPN Routers, except for the dual-image feature of RV082/RV016. The firmware and configuration file are not compatible with earlier hardware versions.

Note:

- A migration utility is available. You can use this utility to convert a configuration file from your old RV0xx router for use on your new RV0xx V3 router.
- A firmware rescue utility is available for recovering the product in case a unit becomes unusable during firmware upgrade.
- If you downgrade the firmware from version 4.0.2.08 to version 4.0.0.07-tm, the MD5 checksum will be 87e627bd93a23a023a419a0fadc435cc and the router will revert to the factory default settings automatically.
- To download the firmware, migration utility, or rescue utility, go to www.cisco.com/go/software, enter the model number of your router in the search box, and click **Find**. Click the appropriate link for the type of file that you want to download, and continue to the download page.

Support for IPv6 Addressing

IPv6 addressing is supported. To enable this feature: Click **Setup > Network** in the navigation tree, select **Dual-Stack IP** in the *IP Mode* section, and then click **Save** to apply your changes. You can then use the features described below.

- **Setup > Network**

  Click the **IPv6** link above the *LAN* section to enable the IPv6 data input fields for the LAN, WAN, and DMZ interfaces (if applicable). Then follow the normal procedures to enter the settings. Refer to the Help as needed. To view the IPv4 data input fields, click the **IPv4** link.

- **System Summary**

  When IPv6 is enabled, the *System Summary* page *System Information* section displays the IPv6 Prefix. The *WAN Status* section displays the full IPv6 address.

- **Setup > Advanced Routing**

  On the *Setup > Advanced Routing* page, click the **IPv6** link near the top of the page to view the IPv6 data input fields in the *Static Routing* section.

- **Setup > IPv6 Transition**

  When IPv6 is enabled, a 6to4 tunnel is enabled by default for IPv6 packet via 6to4 source/destination addressing exchange. This feature allows the router to establish auto-tunnel in IPv4 network (or a real IPv4 Internet connection) across two independent IPv6 networks. You can disable or enable this feature on the *Setup > IPv6 Transition* page.

- **DHCP > DHCP Setup**

  Use the tabs at the top of the page to view and edit the IPv4 or IPv6 settings.

  Note: The following features are not supported for IPv6:

  - DHCPv6 Relay
  - WINS Server
  - Creating a static IP-to-MAC address list, blocking/allowing access by using a static IP-to-MAC address list

- **DHCP > DHCP Status**

  Use the tabs at the top of the page to view the IPv4 or IPv6 status information.

- **Firewall > Access Rules**

  Use the tabs at the top of the page to view and edit the IPv4 or IPv6 access rules.

- **System Management > SNMP**

  If you enable SNMP, you can enter an IPv6 address for the SNMP trap destination.

Resolved Issues

- Fixed an issue in which the Port Triggering range did not work.
- Fixed a MAC clone issue with RV042.
- Fixed an issue in which the nslookup diagnostic utility within the web-based configuration utility could not resolve names in the Local DNS Database.
- Fixed an issue in which ProtectLink-blocked sites caused a download prompt to appear in Firefox and Safari browsers.

Known Issues

- PPTP clients on iPhone/iPad/Mac cannot connect to the PPTP Server on RV0xx V3.
- When a configuration file is imported from another router, the WAN port MAC address is overwritten with the WAN port MAC address of the other device. To undo this effect, go to the *Setup > MAC Address Clone* page, and enter the correct MAC address of the router. The correct MAC address is displayed next to the *User Defined WAN MAC Address* field, as the Default address.
- Forwarding port 80 or 443 to a web server in the LAN of RV0xx V3 does not work when HTTPS is enabled. Please use other ports as a temporary workaround. Alternatively HTTPS can be disabled, but this will disable QuickVPN at the same time.

- The list of default services for Access Rule configuration does not include Ping (ICMP).
- IPSec ESP Wildcard Forwarding is not supported.
- The web-based configuration utility does not display correctly in Firefox version 4. As a work around, use Internet Explorer or Safari.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Cisco Small Business Firmware Downloads	www.cisco.com/go/software
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Product Documentation (Quck Start Guide, Administration Guide, Safety Information)	
Cisco Small Business Routers	www.cisco.com/go/smallbizrouters
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

OL-24758-02