Release Notes for Cisco RV0xx Series VPN Routers Firmware Version 4.1.0.02

November 2011

This document describes resolved issues and known issues in Cisco RV0xx Series Firmware Version 4.1.0.02.

Contents

Contents, page 1

Resolved Issues, page 1

Known Issues, page 2

Support for IPv6 Addressing, page 5

Related Information, page 7

Resolved Issues

- Fixed an issue in which the web-based configuration utility did not display correctly in Firefox version 4. (CSCtq83745)
- Fixed a packet logging issue in which enabling the "Deny Policies" logging option resulted in false “Policy Violation” log entries for TCP/UDP packets that were not in fact dropped.
- Fixed issues in which RV016v3 did not support VPN backup, Split DNS over a gateway-to-gateway VPN tunnel, and transparent bridge.
- Fixed an issue in which the NULL option of Phase 2 authentication was not working for gateway-to-gateway VPN tunnels.

- Fixed an issue in which enabling the "Use Remote DNS Server" option in the Cisco QuickVPN client resulted in DNS name resolution failures over a tunnel to a Cisco RV0xx router.
- Fixed an issue with PPPoE usernames containing the % character. The % character now is accepted.

Known Issues

Read the following information before upgrading the firmware.

Login Error after Upgrading issue

- **Description—**After the router is upgraded to firmware version 4.1.0.02, the router may not accept your existing login credentials. The web browser displays "404 Not Found: The requested server-side includes file names that do not seem to exist."
- **Work Around—**Reboot the router to restore access to the configuration utility.

NAT Traversal with Client To Gateway VPN issue

- **Description—**When a client-to-gateway VPN tunnel is configured in Tunnel mode, the *VPN > Client To Gateway* page does not provide the NAT Traversal option in Advanced Settings. As a result, the VPN client cannot create a tunnel to the gateway.
- **Work Around—**When creating or editing the Client To Gateway settings, choose Group VPN instead of Tunnel. Alternatively, configure a Gateway To Gateway VPN tunnel instead. Both of these options allow you to enable NAT Traversal in Advanced Settings.

IPv6 DHCP Server issue

- **Description—**The IPv6 DHCP server does not re-initialize after the router is rebooted. As a result, the clients lose their stateful IPv6 addresses.
- **Work Around—**To force the router to reinitialize the IPv6 DHCP server, complete these tasks: On the *Setup > Network* page, *IP Mode* section, select **IPv4**, and then click **Save** to apply your changes. Now select **Dual-Stack IP**, and click **Save**.

Keep Alive after Power Cycle issue

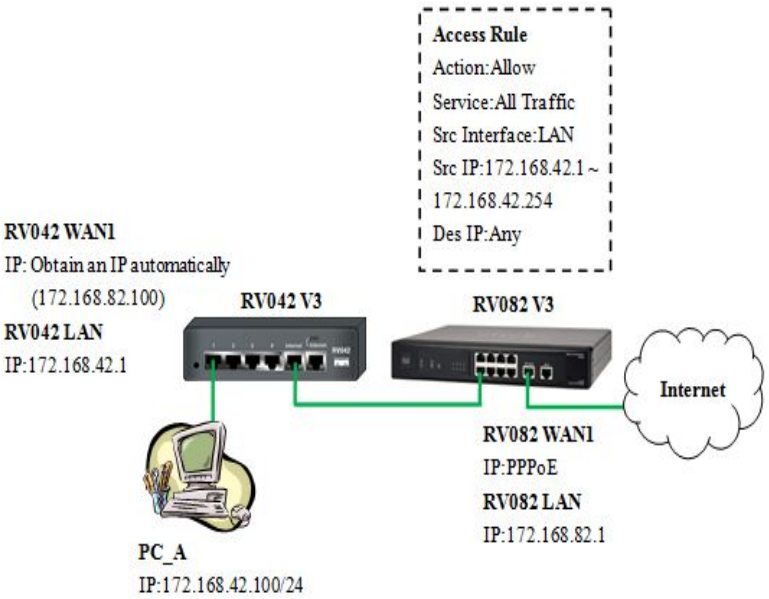
- **Description—**Although Keep Alive is enabled, a gateway-to-gateway tunnel does not automatically reconnect after a router is power-cycled on one end of the tunnel.
- **Work Around—**On the *VPN > Summary* page, click **Disconnect** to disconnect the tunnel. Then allow the tunnel to reconnect through Keep Alive.

Dynamic DNS Host Name issue

- **Description—**On the *Edit Dynamic DNS Setup* page, the configuration utility allows only a 15-character Dynamic DNS host name, although longer host names may be issued by the Dynamic DNS service.
- **Work Around—**None.

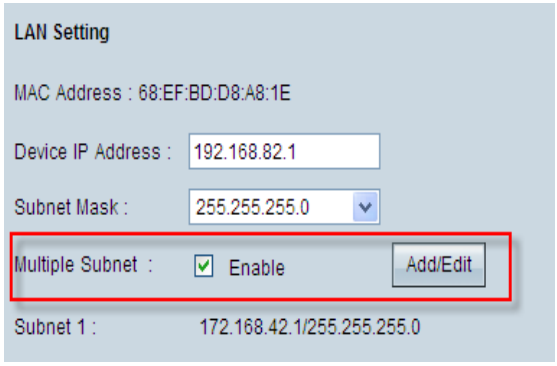
Multiple subnets on LAN issue.

- **Description**—The RV0xx version 3 routers handle multiple subnets on the LAN side differently than the RV0xx version 2 routers. For example, the illustration below shows a sample network where the RV082 v3 (running in Gateway Mode, with NAT enabled) is the internet gateway and the RV042 v3 running in Router Mode is connected to the RV082 v3. To allow the computers in the LAN of the RV042 v3 to access the Internet, you need to add an Access Rule.



- **Workaround**—Add an access rule; for example, in the previous network example, the access rule would be configured as shown below:

NOTE If the router connected to the Internet is an RV0xx v2 model, you need to enable the Multiple Subnet option in the **Setup** > **Network** page of the Management Interface, and enter the LAN subnet of the RV042 v3 into the multiple subnet list of the RV082 v2, as shown below:



Hostname Conflict Resolution issue

- **Description**—If the Cisco RV0xx hostname is modified using the **Setup** > **Network** > **Hostname** page to a name that already exists in the local network, a new Bonjour hostname is generated, but the hostname is not changed.
- **Work Around**—Add a unique MAC extension to the hostname to avoid conflict.

Universal Plug and Play (UPnP) issue

- **Description**—Device description is shown as “Linux Gateway Device” when UPnP is enabled.
- **Work Around**—None.

Support for IPv6 Addressing

IPv6 addressing is supported in firmware version 4.0.2.x and later. 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** tab 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** tab.

  To configure private prefixes: To configure private prefixes, click the **IPv6** tab and then go to the *LAN Settings* section.

  To configure public prefixes: Click the **IPv6** tab, and then click the **Edit** icon for the WAN interface. Towards the bottom of the IPv6 WAN setting page, you will be able to see the IPv6 LAN prefix. You can enter your global/public prefix for your LAN devices.

- **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** tab 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.

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/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/go/software Select a link to download firmware for Cisco Small Business Products. No login is required.
Product Documentation	
Cisco Small Business RV Series 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-26196-01