Release Notes for Cisco RV220W Firmware Version 1.0.4.17

August 2012

These Release Notes describe the changes and known issues in Cisco RV220W firmware version 1.0.4.17.

IMPORTANT:

As with any firmware release, please read these release notes before upgrading the firmware. Cisco also recommends backing up your configuration before any firmware upgrade.

NOTE If you install firmware version 1.0.4.x and later need to revert to a previous firmware version (for example, 1.0.3.x), you must perform a factory reset during the downgrade. If you do not perform a factory reset when downgrading, future upgrades to firmware versions 1.0.4.x will fail.

Contents

This document includes the following topics:

Issues Resolved Since RV220W Firmware Version 1.0.3.5

Tracking #	Description
CSCtk66428	Fixed an issue in which the router allowed configuration of 1-to-1 NAT service only on VLAN1, not on other VLANs.
CSCtl09244	Fixed an issue in which a client’s firewall rules/filters no longer worked after the client was added to the IP/MAC Binding table.
CSCtl79849	Fixed an issue in which IPv6 access rules were not supported.
CSCtq44404	Fixed an issue in which the DHCP Client Table did not show all clients.
CSCtq84421	Fixed an issue in which enabling Daylight Savings Time in the Central European time zone did not display the correct time.
CSCtr00764	Fixed a display issue on the *Administration > Firmware Upgrade* page.
CSCtr12458	Fixed an issue in which the router was leaking RIP packets on the WAN side when set to gateway mode.
CSCtr23433	QuickVPN client cannot access the computers in the LAN of the RV220W when the LAN subnet is smaller than a /24 subnet.
CSCtr24294	Fixed an issue in which the *Status > View Logs* page did not display log entries correctly in Internet Explorer 9.
CSCtr39253	Fixed an issue in which the router failed to apply trusted or self-signed SSL certificates to HTTPS sessions.
CSCtr76367	Adjusted the *URL Filtering Filtered Categories* table on the *Cisco ProtectLink Web > Web Protection* page to display correctly in Internet Explorer 9.
CSCtr83966	Fixed an issue in which a syslog server received only kernel messages.
CSCts00209	Fixed an issue with firewall port-forwarding rules for Internet NAT redirection.
CSCts38114	Fixed an issue in which large file transfers caused a VPN connection failure when using Shrewsoft or TheGreenBow client-to-gateway software.

Tracking #	Description
CSCtt06082	Fixed an issue in which the WAN Traffic Meter did not display correct statistics.
CSCtt08533	Fixed an issue in which port forwarding did not function as designed for a default service after the default value of the source port was changed.
CSCtt22105	Fixed an issue in which VLANs created with firmware version 1.0.1.0 or earlier failed when upgrading to version 1.0.2.4 or later.
CSCtt70054	Fixed an issue in which Daylight Savings Time did not take effect until the router was rebooted.
CSCtw50531	Fixed an issue in which an IPSec VPN peer could not access the web configuration utility if port 80 was forwarded.
CSCtx98521	Fixed an issue in which enabling content filtering caused MAC filtering to fail.
CSCty43634, CSCts38848, CSCts41444	Fixed an issue in which disabling the radio settings did not disable the active access points.
CSCtz04685	Fixed an issue in which a router could not be accessed by using its IPv6 address.

Known Issues in Version 1.0.4.17

The following issues are known to occur in this version of the firmware. Read this information before upgrading.

Logging issues

- Certain syslogs such as IKE and Kernel logs will appear with the time stamp of 2000-01-01 and not the current time. (CSCtu34004)
- The syslog does not always list the timestamps in sequential order. (CSCtu34011)

VPN issues

- Split DNS for IPSec VPN tunnel does not work. (CSCty11096, CSCub34672)
  Work Around: On the *Networking > LAN (Local Network) IPv4 LAN* page, disable DNS Proxy. Specify a valid server on the local network as the Primary DNS and specify a DNS server in the remote VPN peer network as the Secondary DNS.

- A client cannot connect via SSL VPN with a corporate proxy setting. (CSCto14499)
  Work Around: Disable the proxy setting or set the proxy by using the IP address instead of the domain name. For example, in Internet Explorer, adjust the proxy settings by going to **Tools > Internet Options**. Click the **Connections** tab, and then click the **LAN settings** button. Proceed as needed:

  - To disable the proxy, uncheck the **Use a proxy server** box and then check the **Automatically detect settings** box. Click **OK** to save the changes, and then click **OK** to close the *Internet Options* window.

    OR

  - **To identify the proxy by IP address:** Check the **Use a proxy server** box, delete the domain name if in use, and enter the IP address of the proxy server in the **Address** box.

- VPN connectivity can be lost when using SSL VPN port forwarding and later versions of Firefox. (CSCtj59663)
  Work Around: Use Internet Explorer or Firefox version 3.6.17.

- SSL VPN is not working for users with the Windows 7 64-bit operating system. (CSCtq79042)
  Work Around: You have several options:

  - Use Windows XP 64-bit or Windows 7 32-bit.

  - If you wish to continue using Windows 7 64-bit, download and install the Visual C++ 2005 service pack. Use this link: http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=3387

  - Adjust the settings in Internet Explorer as described below.

    1. In Internet Explorer, go to **Tools > Internet Options**.

    2. Click the **Security** tab, and then click the **Custom Level** button.

3. Scroll down to **ActiveX controls and plug-ins**.

4. For **Automatic prompting for ActiveX controls**, click **Enable**.

5. For **Download signed ActiveX controls**, click **Enable**.

6. Click **OK** to save the changes, and then click **OK** to close the Internet Options window.

- When a Gateway To Gateway tunnel is configured in aggressive mode, the router cannot establish a connection to a Cisco RVS4000 or Cisco WRVS4400N router with a dynamic WAN IP address. (CSCtt61631)
  Work Around: Configure a Gateway To Gateway tunnel in Main mode instead. On the *VPN > IPsec > Advanced VPN Setup* page, select the tunnel and then click **Edit**. Change the Exchange Mode to Main. When the VPN tunnel is configured in Main mode, the router can establish a connection. However, be aware that you will need to update the tunnel configuration whenever there is a change in the RVS4000's dynamic IP address.

Wireless issues

- The online help file for Wi-Fi Multimedia (WMM) should read "WMM: Opens the **QoS Configuration** page to edit the QoS configuration parameters for this profile." (CSCtk66482)

- WLAN clients fail to connect to the router using WPA Enterprise or WPA2 Enterprise. (CSCtj76452)
  Work Around: To work around this issue, disable the Block Fragmentation option in the Firewall page.

Other issues

- The GUI configurations listed below require restarting the RV220W. (CSCtu33997)

  - Changing the time zone to use an NTP server.

  - Manually setting the time.

  - Enabling and configuring remote management.

- A 6to4 tunnel may encounter packet loss depending on the type of NIC used. (CSCtr08162)

- SNMP MIBs only support read access. (CSCtj48019)

- WAN QoS profile binding based on a particular services, such as FTP, may not work properly. (CSCtu07893)

Work Around: Select ANY as the service type when creating QoS profiles. This work around limits QoS bindings to the traffic selector match type (IP address Range, MAC address, VLAN, DSCP, and SSID) rather than service type. Due to this limitation you cannot overlap a particular traffic selector match type among the different QoS bindings.

- When specifying the configuration file for Option 67, the *Networking > LAN (Local Network) > Advanced DHCP Configuration* page only allows selection of files with a .cfg extension. (CSCua43166)
- After disabling DHCP on the default VLAN1, the administrator cannot enable Static DHCP on another VLAN. An error message appears: *Please enable DHCP in IPv4 Local Network Page to configure this page.* (CSCtx57621)
  Work Around: If you need to disable DHCP on one VLAN, use a VLAN other than VLAN1.
- Current implementation of DHCP Option 66 does not support an IP address. (CSCua43141)
  Work Around: Use Option 150 or enter a hostname (without a domain name) instead of an IP address when entering the settings on the *Networking > LAN (Local Network) > Advanced DHCP Configuration* page.
- The router does not allow you to append the domain to a hostname when configuring DHCP Option 66. For example, the router will accept "MyHost" as a host name but not "MyHost.example.com" (CSCua43159)
  Work Around: Use DHCP Option 150 instead.
- Static DHCP does not perform consistently. (CSCty43479)
  Work Around: If a PC needs a static IP address, set it on the computer by configuring the adapter settings for the connection.

Firmware Upgrades and Downgrades

Refer to the following instructions:

- Upgrading the Firmware
- Downgrading the Firmware

Upgrading the Firmware

STEP 1 As a best practice before upgrading, back up the current configuration by performing the following tasks:

a. Open the *Administration > Backup / Restore Settings* page.

b. Click the **Backup Startup Configuration** button, and choose a file location. Later, if needed, you can restore the configuration.

STEP 2 On the *Administration > Firmware Upgrade* page, click **Browse** and then select the new firmware.

STEP 3 Click **Upload**.

STEP 4 When the confirmation message appears, click **OK** to continue, or click **Cancel** to close the message without upgrading the firmware.

Downgrading the Firmware

If you wish to re-install an earlier version of the firmware after upgrading, use this procedure.

STEP 1 As a best practice before downgrading, back up the current configuration by performing the following tasks:

a. Open the *Administration > Backup / Restore Settings* page.

b. Click the **Backup Startup Configuration** button, and choose a file location. Later, if you upgrade the firmware, you can restore the configuration.

STEP 2 Check the **Reset all configuration / settings to factory defaults** box.

IMPORTANT: It is necessary to factory reset the router when downgrading the firmware. Checking this box eliminates the need to do a manual reset.

STEP 3 On the *Administration > Firmware Upgrade* page, click **Browse** and then select the firmware that you want to install.

STEP 4 Click **Upload**.

STEP 5 When the confirmation message appears, click **OK** to continue with the downgrade, or click **Cancel** to close the message without modifying the firmware.

STEP 6 To restore the configuration that you saved with the earlier version of the firmware, perform these tasks:

a. Open the *Administration > Backup / Restore Settings* page.

b. Click **Browse** and then select the configuration file.
IMPORTANT: Ensure that the restored configuration file is from the same firmware version that you installed in this procedure.

c. Click **Restore** to restore the saved settings.

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/smallbizfirmware Select a link to download firmware for Cisco Small Business Products. No login is required. Downloads for all other Cisco Small Business products, including Network Storage Systems, are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
Product Documentation	
Cisco RV220W	http://www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
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

78-20941-01