Release Notes for Cisco RV220W Firmware Version 1.0.5.8

December 2013

These Release Notes describe the changes and known issues in Cisco RV220W firmware version 1.0.5.8.

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 1.0.5.x and later need to revert to a previous firmware version (for example, 1.0.4.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 1.0.5.x will fail.

Contents

This document includes the following topics:

Issues Resolved in Version 1.0.5.8

Tracking #	Description
CSCtu02863	Fixed an issue where IPv6 addresses were not handed-off correctly by DHCPv6.
CSCua43166	Fixed an issue where 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.
CSCua43141	Fixed an issue to allow DHCP Option 66 to support an IP address.
CSCub04225	Fixed an issue where the log displayed error strings after upgrading from firmware version 1.0.3.5 to version 1.0.4.17.
CSCtx57621	Fixed an issue in which after disabling DHCP on the default VLAN1, the administrator is not able to enable Static DHCP on another VLAN.
CSCua43159	Fixed an issue in which the device does not allow users to append the domain to a hostname when configuring DHCP Option 66.
CSCub38392	Fixed an issue in which option 150 only supported a singleTFTP server.
CSCuc69361	Fixed an issue to allow users to block URLs by IP address.
CSCud89589	Fixed an issue to allow users to add more than 19 addresses to wireless MAC filter.
CSCua73864	Fixed an issue to prevent the device from rebooting when users upgraded from firmware version 1.0.3.5 or from 1.0.4.11.
CSCuf82085	Fixed an issue to support QoS Rate Limit by SSID.
CSCub19744	Fixed an issue to support QoS Rate Limit by VLAN.
CSCug83521	Fixed an issue prevent the client device on the WAN from accessing the router's LAN IPv6 gateway address.
CSCua39729	Fixed an issue to prevent users from remote managing the device using the IPv6 address from the Internet.

Tracking #	Description
CSCug78836	Fixed an issue to allow users to browse the internet faster a PPTP tunnel when the WAN ISP type is PPPOE.
CSCuj13269	Fixed an issue in which the device displayed an invalid IP address on the Static Route page where the fourth octet is 0 or 255.
CSCui21629	Fixed an issue in which the device displayed an invalid address for the starting IP address in the DHCP pool and for the static DHCP client.
CSCul01468	Fixed an error to support ISATAP tunnels on the device.
CSCuj23441	Fixed an issue in which guest VLAN management is disabled when the device is rebooted.
CSCtk06795	Fixed an issue in which WDS bridging failed to connect when multicast traffic was initiating.

Known Issues

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

Caveats Acknowledged in Release 1.0.5.8

- The Device is unable to send out email logs if it is configured to use a non-default logging policy. (CSCuj85135)
  Workaround: Use the default logging policy.
- 802.1X does not work on the device. (CSCuj86918)
  Workaround: None.
- The total WAN (Internet) bandwidth limiting does not work correctly. (CSCul07244)
  Workaround: Use QoS profile rules to limit the stream bandwidth.
- The total WAN (Internet) bandwidth is 100Mbps and not 1000Mbps. (CSCul07183)
  Workaround: Use QoS profile rules to limit the stream bandwidth.

- QoS Scheduling by priority does not work. (CSCul14468)
  Workaround: None.
- When users change the IPv6 WAN to DHCP mode from static address mode, the WAN status down. (CSCul88869)
  Workaround: Reboot the device after you change the configuration.

Issues Carried Over from Release 1.0.4.17

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

- 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.
-

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

OL-31273-01