Release Notes for RV220W Firmware Version 1.0.2.4

Updated Oct. 13, 2011

These Release Notes describe the changes and known issues in RV220W firmware version 1.0.2.4.

Revisions

Date	Revision
Oct. 13, 2011	Added a known issue: The number of QuickVPN Client users supported is limited to 10 instead of 25.

Contents

This document includes the following topics:

Changes Since RV220W Firmware Version 1.0.1.0

Additions

- **Setup Wizard for quick configuration:** After logging on to the configuration utility, click **Run Setup Wizard** in the navigation tree. Follow the on-screen instructions to set up the Cisco RV220W.
- **Firewall options:** You can now reorder the rules in the *Firewall > Access Rules* table. The rules at the top get enforced before the rules at the bottom. For example, you can place generally applicable rules near the bottom of the table and place exceptions to those rules at the top of the table. See the *Firewall > Access Rules* page.
- **SSH:** SSH is now included in the default list of services to use when configuring features such as firewall access rules and port forwarding rules.
- **Port Statistics:** A new *Status > Port Statistics* page displays current statistics on the number of frames, packets, and bytes that were sent and received through each port.
- **VLAN-based remote management:** You now can allow or block access to the web-based Configuration Utility based from specified VLANs. See the *Networking > LAN (Local Network) > VLAN Membership*.
- **Remote configuration from a TFTP server:** You can configure the Cisco RV220W to download a configuration file from a TFTP server by using Option 66, Option 67, and Option 160. You also can associate different client devices with different configuration files. See the *Networking > LAN (Local Network) > Advanced DHCP Configuration* page.
- **Open port information:** On the new *Status > View Open Ports* page, you can view the following information about open ports: protocol, bytes in the receiving and send queues, the IP address and port for the local and remote clients, the state of the port, and the process that is using the port.
- **Split DNS:** When enabled, this feature allows the Cisco RV220W to find the DNS server of the remote router without going through the ISP's network. See the *VPN > IPsec > Advanced VPN Setup* page.

- **Status dashboard:** The new *Status > Dashboard* page provides summary information about the router, firmware, interface addresses and states, resource utilization, syslog messages, VPN connections, and Cisco ProtectLink licenses.
- **Logging policies:** The Cisco RV220W now supports the configuration of logging policies. You can use the *Administration > Logging > Logging Policies* page to configure multiple logging policies to collect different sets of data. You can use these policies when viewing the logs on the *View > Logs* page, and when sending files to a Syslog server (see the *Administration > Logging > Remote Logging Configuration* page).
- **IPsec VPN Traffic Statistics:** The *Status > IPsec Connection* page now includes statistics for received data as well as transmitted data.
- **SNMP:** SNMP Entity MIB is supported.

Resolved Issues

- Fixed an issue in which a router with a PPPoE connection lost connectivity after the firmware was upgraded.
- Corrected an error that allowed website blocking to be bypassed by using Google Search.
- Fixed an issue with IPv6 6-to-4 tunneling and default dynamic routing.
- Fixed an issue in which a disabled inter-VLAN routing destination continued to receive incoming traffic.
- Corrected a problem with the firewall settings when blocking proxy server access.
- Fixed an issue in which enabling a PPTP server changed the port forwarding Source IP Address to the LAN IP address of the router instead of the IP address of the device that was used to access the service.
- Fixed an issue in which the router lost its IP address and could not recover it, after the network cable was disconnected.

Known Issues in Version 1.0.2.4

- The number of QuickVPN Client users supported is limited to 10 instead of 25.

- A 6to4 tunnel may encounter packet loss depending on the type of NIC used.
- When Internet Explorer version 9 is used, the *Status > View Logs* page does not include line breaks between system log entries.
  Work Around: Use Firefox or Chrome to launch the Configuration Utility.
- On the *Administration > Firmware Upgrade* page, the Firmware Last Updated field is blank.
- SSL VPN is not working for users whose computers are running Windows 7 64-bit.
  Work Around: Use Windows XP 64-bit or Windows 7 32-bit.
- If a client has its IP address bound to a MAC address in the IP/MAC Binding table, firewall rules/filters enabled for the client no longer work. All traffic is allowed to pass through this client even though IP blocking/filtering for the client is enabled on the RV220W.

  Work Around: Do not use IP/MAC Binding for a client that has firewall rules/filters assigned to it.
- The following GUI configurations require restarting the RV220W:
  - Changing the time zone to use an NTP server.
  - Manually setting the time.
  - Enabling and configuring remote management.
- 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.”
- SNMP MIBs only support Read access.
- VPN connectivity can be lost when using SSL VPN port forwarding and later versions of Firefox.
  Work Around: Use Internet Explorer or Firefox version 3.6.17.
- WLAN clients fail to connect to the router using WPA Enterprise or WPA2 Enterprise.
  Work Around: To work around this issue, disable the Block Fragmentation option in the Firewall page.
- Known open issue with enabling the Aggressive mode for IPSec VPN.
  Work Around: Use the Main mode instead.
- The DHCP Client Table does not show all clients.

- NTP stops working after upgrading from firmware version 1.0.1.0 to 1.0.2.4.
  Work Around: Factory reset the router.
- Certain Syslogs such as IKE and Kernel logs will be shown with the time stamp of 2000-01-01 and not the current time.
- The Syslog does not always list the timestamp in sequential order.
- The router fails to apply trusted or self-signed SSL certificates to HTTPS sessions. Although on-screen messages indicate that the certificate was successfully added, the router uses the original default certificate for subsequent HTTPS connections.
  Work Around: The router will use a certificate that is signed by root CA. You can generate a Self Certificate Request from the router and have it signed by the root CA. Upload the root CA certificate in the Trusted CA Certificate table. Finally, upload the signed certificate in the Active Self Certificate table. See the *Security > SSL Certificate* page.
- Internet NAT redirection does not work using firewall port-forwarding rules. A LAN client cannot access a service by using the WAN IP address of the LAN device (such as an IP camera or an FTP server).
  Work Around: Do not use the *Firewall > Port Forwarding* page, but instead create the forwarding rule by using the *Firewall > Access Rules* page. The working port forwarding entry is created along with the firewall access rule.
- A critical error is encountered when attempting to configure settings for remote logging to a syslog server.
  Work Around: Enable email logging on the *Administration > Logging > Remote Logging Configuration* page.
- A client cannot connect via SSLVPN with a corporate proxy setting.
  Work Around: Disable the proxy setting or set the proxy 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.

- There are issues with the SSL VPN client installer on Internet Explorer 8.
  Work Around: 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.

- A client cannot connect via SSLVPN when using MacOs+Java 1.6.0.26.
  Work Around: Downgrade Java version and use FireFox version 3.16.
  Follow the procedure described below to downgrade Java and Firefox.

  1. Login to your MacIntosh computer as administrator.
  2. Start the terminal: Finder> Applications > Utilities > Terminal.
  3. At the command prompt enter these commands:

     ```
     user1% sudo passwd root

     Enter Password:

     Changing password for root

     New password:
     ```

     Verify password:

     The “root” account is enabled after the above steps.
  4. Log out of your current account.
  5. Re-login and at the prompt, enter your “root” username and password that you've just created.

6. Check Java version: Finder> Applications > Utilities > Java Preferences.

   If Java version is 10.6.0.24 or higher, go here to download and then install earlier version of Java: http://www.uploadstation.com/file/a44a57U/JavaforMacOSX10.6Update1Downgrade.zip

   If the install is successful, continue to the next step. If your computer does not allow to install of older Java version, open a Terminal session (Finder> Applications > Utilities > Terminal) and enter these commands to bypass checking Java version during installation:

   ```
   root% cd /System/Library/Frameworks/JavaVM.framework/Resources
   root% mv Info.plist Info.plist.orig
   root% mv version.plist version.plist.orig
   ```

7. Download FireFox v3.16 for MacOs from this site: http://www.mozilla.com/en-US/firefox/all-older.html
8. Install the FireFox 3.16. (Enter “root” password if asked)
9. Open the FireFox browser, and log into the router as SSLVPN user. The portal page appears.

Firmware Upgrades and Downgrades

Refer to the following instructions:

- **Upgrading from 1.0.1.0 to 1.0.2.4**
- **Downgrading from 1.0.2.4 to 1.0.1.0**

Upgrading from 1.0.1.0 to 1.0.2.4

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 file for firmware version 1.0.2.4.

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 from 1.0.2.4 to 1.0.1.0

If you wish to re-install firmware version 1.0.1.0 after upgrading to firmware version 1.0.2.4, 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 for version 1.0.1.0.

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 previously, 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 version 1.0.1.0.

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-24250-02