

Release Notes for WRVS4400N V1.0 and V1.1 Firmware Version 1.1.13

2/24/2009

These Release Notes describe the resolved issues and updates in the WRVS4400N V1.0 and V1.1 firmware version 1.1.13.



NOTE

Due to the updated code added in this new release, the configuration file of an earlier firmware cannot be used after the firmware is upgraded to v1.1.13. Please reset the router to the factory default after the upgrade.

Firmware Version 1.1.13 can only be used with a WRVS4400N V1.0 or V1.1. Do not use the 1.1.13 firmware image with a WRVS4400N V2.

Be sure to backup your configuration file first in case you want to revert the firmware back to an earlier version.

Contents

This document includes the following topics:

- **“Downloading the New Firmware,” on page 2**
- **“WRVS4400N V1.0 and V1.1 Firmware Version 1.1.13,” on page 2**
- **“WRVS4400N V1.0 and V1.1 Firmware Version 1.01.03,” on page 5**
- **“WRVS4400N V1.0 and V1.1 Firmware Version 1.00.16,” on page 6**
- **“WRVS4400N V1.0 and V1.1 Firmware Version 1.00.15,” on page 6**
- **“WRVS4400N V1.0 and V1.1 Firmware Version 1.00.13,” on page 7**

- “**WRVS4400N V1.0 and V1.1 Firmware Version 1.00.12,”** on page 7
- “**Related Information,”** on page 8

Downloading the New Firmware

To download the new firmware, go to:

<http://www.cisco.com/en/US/products/ps9931/index.html>

Click on the **Download Software** link under Support.

Cisco WRVS4400N Wireless-N Gigabit Security Router - VPH

Introduction

Secure and Speedy Wireless Networking

Complicated applications need a bigger network pipe for better performance. Formerly Linksys Business Series, now Cisco Small Business Routers, the WRVS4400N Gigabit Security Router offers next-generation Wireless-N speeds while maintaining compatibility with older devices. The router's "multiple-in, multiple-out" (MIMO) technology extends its range and performance.

The WRVS4400N incorporates advanced security features to keep your network safe from external threats like viruses, spyware, and hacker attacks. Offsite workers can access your network through a secure and easy-to-use virtual private network (VPN) function.

Additional features of the WRVS4400N Gigabit Security Router include:

- A 4-port Gigabit Ethernet switch for maximum wired performance
- QuickVPN utility to minimize setup time for secure VPN tunnels for remote access
- SPI Firewall, and Intrusion Prevention System secure the work from outside threats
- VLAN and RADIUS Authentication support makes your network secure
- Quality of service (QoS) provides best quality voice and video with consistent, high-quality connections



Support

[Download Software for this product.](#)

192611

WRVS4400N V1.0 and V1.1 Firmware Version 1.1.13

Issues Resolved

- Resolved an issue that caused the Quick VPN client to fail to reconnect to the router after disconnecting a VPN session.
- Resolved an issue in Dual-Stack Mode feature that caused the router to not work properly if IPv6 mode was enabled.
- Resolved an issue in the **Administration** -> **Management** tab that caused the router WebGUI to not be able to remove router usernames.
- Resolved an issue in the Web GUI that allowed a user to enter and save an invalid character string in the Syslog Server field.
- Resolved an issue in the Web GUI that allowed a user to save an invalid LAN IP address.

- Resolved an issue that allowed an invalid IP address to be saved in the **Static IP Mapping** tab of the Web GUI.
- Resolved an unclear statement in the popup message after enabling remote management.
- Resolved a typo in the popup message that occurred when a user created the same username to access the router.
- Updated the TrendMicro server certificate for URL, Access, and email security.
- Resolved an issue on the **WebGUI Firewall** page that causes the check boxes to become grayed out after clicking the "Disable All Rules" button.
- Resolved an issue that causes the Wireless AP to become unresponsive after changing Wireless MAC Control from "Prevent" to "Allow."
- Resolved an issue on the **WebGUI Firewall** page. If *any* IP-based ACL rules are present, then any Forbidden Domains or Keywords present in the Internet Access Policy are not applied.
- Resolved an issue on the **Administration-> Log** page that causes the "View Outgoing Table" and "View Incoming Table" buttons to remain grayed out and inaccessible after log settings are saved.
- Resolved an issue in the **Switch QoS Settings** page that causes you to be unable to save the CoS settings.
- Resolved an issue in the WLAN driver that caused connectivity issues with older WLAN adapters. It is recommended that customers update the WLAN client adapter driver version to the latest from the manufacturers website.
- Resolved an issue on the **Firewall -> Basic Settings** page. When customers enabled Block Java, Cookies, ActiveX, or Access to Proxy HTTP Server, websites would open slowly.
- Resolved an issue in Dynamic DNS resolution that causes the VPN tunnel to fail to connect to the new WAN IP if the WAN IP changed.
- Resolved an issue in IPS that causes FTP throughput to become very slow when transferring large quantities of smaller files.
- Updated IPS signature support for version 1.40.
- Resolved an issue in the WebGUI that causes the advanced parameters section of the VPN page to not save the settings.
- Resolved an issue that causes the WebGUI to become inaccessible when being accessed across a QuickVPN tunnel established by a Vista PC.

Release Notes

- Resolved an issue in the VLAN code that causes the switch ports to be unresponsive until a system power cycle is performed.
- Updated PPPoE and L2TP username and password fields to support special characters.
- Updated the pop-up message for the password field when users enter more than 22 characters.
- Updated the setting for "Management via WLAN" to be disabled by default.
- Resolved an issue in the WebGUI to show the accurate amount of VPN tunnels available and in use.
- Resolved an issue in the WebGUI formatting that causes the **Remote Management** page to become unviewable when the user is using Firefox to view the router WebGUI remotely.
- Resolved an interoperability issue between the WRVS4400N and the WET200.
- Resolved an issue in the VPN subsystem that causes the NetBIOS Broadcast to fail across a VPN tunnel.
- Resolved an issue that causes the System UP time shown in the SNMP Browser to not match the System Up time in the WebGUI.
- Resolved an issue that causes the DHCP Server on a VLAN-based subnet to not assign the statically configured DNS Server to the DHCP Clients.
- Resolved an issue that causes Port Forwarded packets to fail to go through the HardwareNAT table when IPS is disabled.
- Resolved an issue when a user applies https (SSL) to do remote management, the packet with SSL port 443 does not get forwarded to the LAN through port forwarding.
- Resolved an issue in the LAN subnet pulldown menu. Removed the 255.255.255.252 subnet.

WRVS4400N V1.0 and V1.1 Firmware Version 1.01.03

Issues Resolved

- Support of 802.1Q VLAN (up to 4) including access/trunk modes on LAN ports and access mode only on wireless interface.
- Support of the following advanced IPv6 features on LAN ports:
 - 6to4 tunnels to connect IPv6 islands through IPv4 Internet
 - 6to4 Access Control List to allow traffic between trusted IPv6 islands
 - Static IPv6 DNS entries for hosts across 6to4 tunnels
 - A DHCP server for IPv6
- Support of Custom DNS provided by DynDNS.org.
- Support of DHCP static IP based on MAC address. Up to 50 entries are supported.
- IPsec VPN now supports a remote gateway defined by a DDNS domain name.
- QuickVPN supports a self-generated certificate on the VPN Client Accounts page.
- QoS supports bandwidth management (layer-3 QoS).
- QoS supports DSCP/CoS/port-based QoS (layer-2 QoS).
- Event logging supports multiple severity levels.
- Email Alert supports SMTP Authentication.
- L2 Switch supports port mirroring and RSTP.
- DHCP Server (in the **Setup** -> **LAN** page) supports multiple subnets, once multiple VLANs are created.
- Routing support between VLANs, that can be enabled/disabled in the **Setup**-> **Advanced Routing** page.
- Support of an option to block management GUI access by wireless clients.
- Updated the IPS Signature file to 1.29.
- Changed the 11n default channel bandwidth to 20MHz.

Release Notes

- US and EU versions are now supported in one firmware. The version booting up will be determined by hardware.
- Support of MS-CHAPv2 for PPPoE authentication.
- WAN IP address validity is now checked based on the subnetmask configured.

Known Issues

- QVPN v1.2.6 (Vista version) behind a NAT router cannot connect to WRVS4400N on the Internet.
- Subnetmask 255.255.255.252 cannot be configured on LAN and it should be removed from the drop-down menu.
- The following feature is not working: NAPT-PT should allow IPv6-only hosts to access IPv4 servers on Internet by hostname.

WRVS4400N V1.0 and V1.1 Firmware Version 1.00.16

Issues Resolved

- Resolved the issue of the QuickVPN connection issue if subnet mask is not 255.255.255.0.

WRVS4400N V1.0 and V1.1 Firmware Version 1.00.15

Issues Resolved

- WLAN to WAN traffic now goes through HNAT. The throughput can be improved from 30+Mbps to over 100Mbps (up to wireless limitation).
- Resolved the issue of when the Remote Security Gateway type was set to *Any*, an alert window would appear. This message would appear even though a name was already entered for Local Identity.
- Unified wireless security keywords to match Linksys Business Series products.

WRVS4400N V1.0 and V1.1 Firmware Version 1.00.13

Issues Resolved

- Allows WPA shared key to take 64 Hexadecimal digits.
- Displays wireless MAC address under **Status** -> **Wireless LAN** page.
- Enhanced the DHCP server to support hostnames of up to 63 characters (was limited to 15 chars).
- Updated the IPS signature file bundled inside the firmware to v1.25.
- Updated expired SSL certificates.
- Updated *WPA Shared Key* GUI term on WPA PSK modes to be consistent with other products.
- Port 443 now goes into stealth mode if no VPN client was configured.
- Resolved the issue that port 443 cannot perform port forwarding (was reserved for QVPN).
- Resolved the issue that single port forwarding cannot work together with IP based ACL to limit external access.
- Enhanced UPnP command checking to prevent illegal packet forwarding.

WRVS4400N V1.0 and V1.1 Firmware Version 1.00.12

Issues Resolved

- Improved UDP HNAT performance.
- Updated IPS signature file bundled inside the firmware to v1.22.
- Now allow NetBIOS traffic to pass through VPN tunnel. This allows Microsoft Windows to search for a computer on the other side of the tunnel.
- Resolved the issue that IP ACL rule could not save if the source IP type was *Any*.
- Resolved the issue that DHCP server address could not save if using DHCP Relay.

Release Notes

- Resolved 802.11n interoperability with Linksys WPC300N (& WMP300N) on WPA2. Please also download latest driver for WPC300N (v4.100.15.5). If using windows XP zero config for WPA2, please download windows hotfix KB893357.

Related Information

Resource	Location
Technical Documentation	http://www.cisco.com/en/US/products/ps9923/index.html
Firmware Downloads	http://www.cisco.com/en/US/products/ps9923/index.html
Customer Support	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Open Source License Notices	www.cisco.com/go/osln
Regulatory Compliance and Safety Information	Regulatory and Safety Information can be found in the WRVS4400N Administration Guide found at the following link: http://www.cisco.com/en/US/products/ps9923/prod_maintenance_guides_list.html
Warranty Information	www.cisco.com/go/warranty
Cisco Partner Central site for Small Business	www.cisco.com/web/partners/sell/smb

Cisco, Cisco Systems, the Cisco logo, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

© 2009 Cisco Systems, Inc. All rights reserved.

OL-19066-01