Release Notes

Firmware 6.3.11

ICR-OS

Abstract

This document encompasses the following key sections:

- **Firmware Update Instructions:** Guides users through the firmware update process, ensuring a smooth and successful experience.

- **Description of New Features, Fixes, and Changes:** Provides detailed information about new features, enhancements, fixes for previous issues, and other significant changes included in the firmware update.

- **Known Issues Related to the Firmware Version:** Informs users about any existing issues or limitations with this firmware version, aiding in informed decision-making and preparation.

Firmware Release Information

- **Version**: 6.3.11

- **Release Date**: February 7, 2024

- **Compatibility and Distribution**: Compatible with a v2 production line of these Advantech router models:

  SPECTRE RT | ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E

  For comprehensive compatibility details and distribution guidelines, see the *Firmware Compatibility Chart* document published with the specific firmware version.

Firmware and Product Documentation Notice

- **Router Configuration Information:** The most recent and detailed configuration information is available in the *Configuration Manual* for your router model.

- **Accessing Documents and Applications:** Visit the *Engineering Portal* at *icr.advantech.com* for product-related documents, applications, and firmware updates.

Contents

Part I.

Firmware Update Instructions

General Update Instructions and Notices

HTTPS Certificates:

- Following the release of firmware version 5.3.5, the router's HTTPS certificate format has been updated to enhance security measures. It is crucial to recognize that routers produced prior to this firmware version will not have their HTTPS certificates automatically updated during the firmware upgrade process.

- For manual HTTPS certificate updates, remove the existing certificate files found at `/etc/certs/https*` on the router. This action should be performed through an SSH connection. The certificates will be automatically regenerated in the new format upon the next reboot of the router.

Part II.

Description of New Features, Changes, and Fixes

Added

CPU & Memory Usage Information

This update introduces a valuable feature for monitoring system performance. Users can now view real-time information regarding CPU and memory usage. This information is readily accessible on the *Status → General* page, specifically within the *System Information* section.

For convenience and to ensure up-to-date information, there is an option for automatic updates. By clicking the *Refresh* button located in the upper right corner of the GUI page, users can enable the interface to update these values dynamically.

RTC Setting from Web UI

The recent enhancement to the Real Time Clock (RTC) feature introduces a convenient way to synchronize the router's clock with the user's web browser time. By simply clicking the *Apply browser time* button (*Administration → Set Real Time Clock*), users can ensure the router's internal clock matches the current time displayed in their web browser. This improvement facilitates an easy and efficient method to maintain accurate time settings on the router.

SIP ALG Suport

The most recent firmware update introduces support for SIP ALG, an abbreviation for *SIP Application-Layer Gateway*. This feature is a significant enhancement for users who rely on multimedia sessions, such as internet telephony calls, facilitated by the Session Initiation Protocol (SIP).

SIP ALG plays a crucial role in the management of SIP traffic, especially in networks utilizing Network Address Translation (NAT). It aids in the establishment, modification, and termination of SIP-based multimedia sessions. By inspecting and modifying SIP packets as necessary, SIP ALG ensures that they navigate through NATing firewalls without issues. This is particularly important in environments where SIP traffic must pass through a firewall or router that performs NAT.

Follow WiFi STA Radio Settings

The introduction of the *Follow STA radio settings* parameter in the Wi-Fi Access Point (AP) configuration marks a significant advancement in network adaptability. This new parameter, when activated, changes the behavior of the Wi-Fi AP to dynamically align its radio settings with those of a foreign AP to which the Station (STA) is connected.

By default, this parameter is disabled, meaning the AP operates as it traditionally has. In this default mode, the AP maintains its predetermined radio settings regardless of the STA's connection status. However, when the *Follow STA radio settings* parameter is enabled, it allows the AP to automatically adjust its radio settings – such as frequency, channel, and other relevant parameters – to match those of the foreign AP currently connected to the STA.

This feature is particularly useful in environments where the AP needs to be flexible and adapt to various network conditions. It ensures a more seamless and efficient network experience, especially in scenarios where the STA frequently connects to different foreign APs with varying configurations.

Profile SNMP OID

The SNMP (Simple Network Management Protocol) OID (Object Identifier) structure in the router has been enhanced with the addition of a new read-only OID, .1.3.6.1.4.1.30140.6.10, labeled as *infoProfile*. This OID is specifically designed to represent the current configuration profile of the router.

The *infoProfile* OID can assume one of four values: *standard*, *alt1*, *alt2*, or *alt3*. These values correspond to the standard configuration profile and three alternative configuration profiles, respectively. This feature allows for easier monitoring and management of the router's configuration state via SNMP.

SNMP for Binary Inputs

The SNMP (Simple Network Management Protocol) configuration has been further enhanced with the addition of entries for the binary inputs BIN2 and BIN3. This update extends the SNMP monitoring capabilities to these specific binary inputs, allowing for more comprehensive network management and monitoring.

Cellular Registration Timeout

A new configuration feature now allows for the customization of the cellular network registration timeout. Although the standard 2-minute timeout suffices for most scenarios, there are specific cases where adjustments are necessary. To cater to such needs, configuration options named `PPP_REG_TOUT`, `PPP_REG_TOUT2`, `PPP_REG_TOUT3`, and `PPP_REG_TOUT4` have been introduced. These options allow for configuring the registration timeouts for the first to the fourth SIM cards, respectively. Expressed in seconds, these settings offer precise control over the network registration timing. Adjustments can be made via the router console or incorporated into startup scripts, though they are not available through the graphical user interface (GUI).

> For experts only. Incorrect usage can lead to system instability or malfunction.

Fixed

Date in Emails

The latest firmware update rectifies an issue related to the router's email functionality, where previously, the date information was absent in the data section of emails produced by the router. This problem has now been effectively resolved.

WiFi Startup

The firmware update includes a crucial fix for the *hostapd* daemon, addressing a previously identified issue where a configuration error was causing the WiFi script to fail to start. This fix rectifies the problem, ensuring that the *hostapd* daemon initiates correctly and operates as intended.

VRRP Ping

The issue with ping functionality in VRRP, where it only worked correctly for *Ping Interval* values less than 4250 seconds, has been resolved. Previously, for intervals over 4250 seconds, the ping occurred continuously, which is no longer the case.

SNMP for Serial Number

A fix has been implemented for an SNMP issue that caused the SNMP get for the serial number to become blocked after any system reboot, whether soft or hard. This problem was resolved after the first login on the WebGUI, but the fix now ensures uninterrupted SNMP functionality post-reboot.

Docker Container Availability Issue

The recent firmware update has successfully addressed the issue with the *Docker* Router App, which was previously unable to install containers. This problem stemmed from an unreachable repository, impeding the App's functionality. With this resolution, the *Docker* Router App can now seamlessly install containers, enhancing its usability and efficiency.

`Ntpdate` Issue

The *ntpdate* command has been updated to fix a buffer overflow issue, enhancing its security and stability.

Licenses List

The issue where the license page in the Web GUI did not display the full list of licenses, especially for Router Apps with many dependencies like Node-RED and their nodes, has been fixed.

SNMP Reporting

The issue where the SNMP item `mobileReportPeriod` (OID 1.3.6.1.4.1.30140.4.22) was not returning any value has been fixed.

Security

Fixed DoS Attack Crash

The firmware update resolves an issue where the *totd* daemon stopped functioning after a DoS attack on the router, affecting DNS address resolution.

Part III.

Known Issues Related to the Firmware Version

Firmware Update – Unexpected Filename

There is a known issue that occurs if the filename of the firmware intended for your router has been altered. This can affect both manual firmware updates and the Automatic Update feature. When encountering this issue, the following warning message is displayed: *"You are trying to upload file 'xx.bin' but 'yy.bin' is expected. Are you sure to continue?"* To resolve this issue, please follow the instructions provided in Part I - Firmware Update Instructions of this document.

WiFi Configuration – Lost After Firmware Downgrade

Be aware that if you downgrade your firmware to a version earlier than 6.2.0, all existing WiFi configurations will be completely lost. It's important to back up your configuration before proceeding with such a downgrade.

ICR-3200 – Country Code for WiFi

In the initial firmware version for the ICR-3200 WiFi module, there is a limitation regarding the setting of the country code. Any modifications to the country code made on the configuration page will not have any effect. This is because the country code for the WiFi module is pre-set during the manufacturing process, based on the intended region of product distribution.

SmartStart – Cellular Network Registration

For the SmartStart router to function optimally with the *Telit* cellular module, it is crucial to use router firmware version 6.1.5 or higher. This requirement applies specifically if your router is equipped with one of the following *Telit* cellular module versions:

  • *Telit LE910-EU V2* cellular module, firmware version 20.00.403 or newer.
  • *Telit LE910-NA1* cellular module, firmware version 20.00.014 or newer.

Note: You can find the model name and firmware version of the cellular module in the router's web GUI, under the *Mobile WAN Status* page, within the *Mobile Network Information* section.

SmartStart SL302 – Cellular Network Authentication

For the SmartStart SL302 router equipped with the Telit LE910-NA1 cellular module firmware version 20.00.522, there is a known limitation: It is not possible to use a username and password for authentication when connecting to the Mobile WAN network. This restriction specifically affects settings configured on the *Mobile WAN Configuration* page.
To check the firmware version of your cellular module, visit the *Mobile WAN Status* page in the router's web GUI, where it is listed under the *Mobile Network Information* section.

SmartStart SL302 – SMS in *Verizon* Network

The SmartStart SL302 router, when equipped with the *Telit* cellular modules *LE910-SV1* or *LE910-NA1*, supports the sending and receiving of SMS messages within the *Verizon* cellular network starting from firmware version 6.1.4. It is important to note that in order to enable the receipt of SMS messages, the cellular module must be running a *Verizon* firmware version higher than 20.00.012.

Incorrect Mobile Data

There is an issue in firmware version 6.3.8 where the mobile interface data retrieved via SNMP or reported by the *R-SeeNet* system may be inaccurate. To resolve this issue, it is recommended to update the router's firmware to a version higher than 6.3.8.