SMART/RG®
forward thinking

/SOFTWARE RELEASE NOTES

Release 2.5.0.8

Relevant Models:
SR350N
SR350NE
SR360n
SR500N
SR500NE
SR505n
SR510n
SR550n
SR552n

June 26, 2015

TABLE OF CONTENTS

DOCUMENT HISTORY

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	12/30/14	Adam Fox	Document Creation

Notice of Document Integrity
The contents of this document are current as of the date of publication. SmartRG Inc. reserves the right to change the contents without prior notice. In no event will SmartRG be liable for any damages or for commercial losses resulting from information contained in this document.

SW REVISION SUMMARY

SW REVISION	DSP/XDSL LINE DRIVER	CFE	WIRELESS DRIVER REVISION	DATE
2.5.0.8	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	6/26/15
2.5.0.7	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	5/19/15
2.5.0.6	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	12/30/14
2.5.0.5	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510) A2pvbF039j.d25d (SR550n/SR552nn)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	10/10/14
2.5.0.4	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510) A2pvbF039j.d25d (SR550n/SR552nn)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	7/7/14
2.5.0.3	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	6/6/14

	A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510) A2pvbF039j.d25d (SR550n)			
2.5.0.2	A2pG038i.d25 (SR360n) A2pD038f.d25 (SR350N) A2pv6C039b.d25 (SR500N) A2pv6F039b.d25 (SR505n/SR510) A2pvbF038n.d25 (SR550n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	4/18/14
2.5.0.1	A2pD038f.d24m (SR350N) A2pG038i.d24m (SR360n) A2pv6C039b.d24m (SR500N) A2pv6F039b.d24m (SR505n/SR510) A2pvbF038n.d24m (SR550n)	1.0.38-114.70	6.30.102.7.cpe4.12L08.0	12/19/13
2.4.4.6	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N) A2pv6F037a.d24a (SR505n)	1.0.38-112.70	5.100.138.2001.cpe4.12L04.3	8/26/2013
2.4.4.5	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N) A2pv6F037a.d24a (SR505n)	1.0.38-112.70	5.100.138.2001.cpe4.12L04.3	6/5/2013
2.4.4.4	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	11/12/2012
2.4.4.3	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	10/11/2012
2.4.4.2	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	7/30/2012
2.4.3.7	A2pD030n.d23c (SR350N) A2pv6C032a.d23c (SR500N)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	5/31/2012
2.4.3.6	A2pD030n.d23c (SR350N) A2pv6C032a.d23c (SR500N)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	4/26/2012

CHANGES AND FIXES

REFERENCE NUMBER	DESCRIPTION
RB-1823	Resolved a migration anomaly with the SR5xx series RGs (when upgrading to 2.5.0.7, the MTU size could be set to Jumbo for GigE interfaces, which could cause Internet connection issues).
RB-1830	Resolved a migration anomaly Advanced WiFi parameters (when upgrading to 2.5.0.7, in some instances, the Passphrase would be overridden by the new SmartRG factory defaults (pseudo-random) Passphrase).
RB-1832	Resolved anomaly when using Serial Number OUI under the TR-069 client (WiFi Passphrase was being overwritten).
RB-1834	Resolved an issue with using a Blank WiFi Passphrase causing the GUI not to display properly.

IMPROVEMENTS

REFERENCE NUMBER	DESCRIPTION
RB-1793	The LCP settings for PPPoE can now be changed after a WAN service has been created via the GUI.

COMPATIBILITY/SYSTEM NOTES

The introduction of Custom Default Settings feature requires the CFE to be upgraded when moving from any firmware version 2.4.4.2 or before. Firmware upgrades from any version below 2.4.4.3 to 2.4.4.3 or newer requires the CFE to be upgraded by use of the firmware that includes a new CFE. Firmware files containing a CFE contain the string “cfe” in the filename. For example, the file, CA_PBCA_2.4.4.3_24742_SR350N_cfe_fs_kernel, would be used to upgrade the firmware on a SR350N gateway.

Failure to upgrade the CFE when moving from a firmware version before version 2.4.4.3 will result in unpredictable operation of the gateway and unknown factory default settings.

Downgrading from 2.4.4.3 and newer versions to pre 2.4.4.3 is not advised. If a downgrade must be accomplished, a factory default of the device via the reset button must be performed. The downgrade must be accomplished using the CFE image of the target firmware release. Factory default the device after the firmware has been downgraded by holding the reset button for at least 10 seconds after applying power to the device. Power must be off before pressing the reset button.

Downgrading from 2.5.0.7 and newer releases is not advised due to the increased configuration size. If a downgrade must be accomplished, a factory default of the device via the reset button must be performed. See the above paragraph for more information.

In order to support expanded configuration files, it is recommended that the SR552n be upgraded to 2.5.0.5 or later. The cfe_fs_kernel image is required for the upgrade. Note that this will result in a factory reset only during the initial upgrade. All subsequent upgrades will retain the configuration.

IGMP Snooping Definitions:

Standard Mode - in standard mode, if multicast traffic is present on a LAN port but no membership report (join) was received, the traffic will flood to all ports. If a membership report was received, multicast traffic will be forwarded only to the LAN ports on which the IGMP membership reports arrived.

Blocking Mode - in blocking mode, multicast traffic will be blocked from all ports until such time a report is received.

If IGMP snooping is disabled the CPE floods multicast packets to all its ports. IGMP Snooping is disabled by default.

This software supports ITU-T G.inp (G.998.4) Physical Layer Retransmission (PhyR) which operates at layer 1 and uses a mechanism similar to TCP where retransmits occur if errors are detected. This results in high effective INP (Impulse Noise Protection) with minimal interleave delay. By enabling PhyR at both DSLAM and CPE, Service Providers can realize improved DSL Showtime rates at lower SNR margins as well as increased robustness and resistance to impulsive noise/interference. PhyR is disabled by default but can be enabled in the DSL menu. For more information about PhyR, please contact your SmartRG Sales Engineering representative.

Wireless is enabled by default with SSID = SmartRGxxxx (x = last four characters of base MAC). Wireless security is Mixed WPA2/WPA-PSK, passphrase is a pseudo-random 10-digit string, Rekey interval = 0 and encryption = TKIP+AES.

Included PBCA Features:

- Control Panel

- Content Filtering
- Time Blocking
- Captive Portal
- Connect and Surf
- STUN and UDP Connection Request
- Advanced Connected Device Monitor
- Bandwidth Monitor
- WiFi Performance Monitor
- Dynamic Content Filtering

Prior FW Releases

Contact SmartRG support for the release notes for prior firmware releases.

FW UPGRADE PROCEDURE

Upgrade Firmware

1. Open a web browser, connect to 192.168.1.1/admin, and login with username **admin** and password **admin** (or customer specific IP address and login info)
2. Click Management → Update Software and select the Browse button.
3. Locate and select the appropriate firmware image.
4. Select the Update Software Button. The image will be uploaded to the device and the device will automatically reboot upon completion.

Verify

1. Hit the F5 Key to refresh your browser and reconnect to 192.168.1.1/admin to log back into the device.
2. Click on Device Info.
3. Verify the version information in the *Software Version* field.

Restore Defaults

1. Click on the Management Link
2. Click on settings.
3. Click on Restore Default.

CUSTOM DEFAULTS

The Custom Defaults feature allows the importation of a set of defaults to the gateway that will be restored when the Restore Default Settings is activated. This set of defaults can be defined and updated via the GUI, CLI or CWMP support of the gateway.

To create a set of Custom Default settings, configure the gateway as required. Use the Backup Running Configuration button on the Backup Settings to upload a configuration file from the gateway. After the file is uploaded, choose the file and use the Update Working Settings button on the Update Settings window to download the file to the gateway. The gateway will use the downloaded settings as the custom default whenever the Restore Default operation is invoked.

TECH SUPPORT:

CPE Issues:

Submit a ticket using our Customer Portal at https://smartrg.atlassian.net

RMAs:

Open a Customer Portal ticket with description "RMA" and attach a spreadsheet which includes Model, MAC address, Issue, and Firmware version.

Firmware:

Login to the Customer Portal to download firmware.

Additional Contact Info:

Phone: +1 360 859 1780, Option 4 Hours: 5am –5pm PST (UTC-0800) Email: support@smartrg.com