



Software Release Notes

Release 2.4.4.5

Relevant to SR Series Models:

SR350N SR350NE

SR500N SR500NE

SR505N

Document History

Version	Date	Author	Description
1.0	08/05/2012	M. Solomon	Document creation
2.0	10/11/2012	P. Franzek	Addition of Custom Defaults Usage

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 Version	DSP/xDSL Line Driver	CFE	Wireless Driver	Release Date
2.4.4.5	A2pD035j.d24a (SR350) A2pv6C035j.d24a (SR500) A2pv6F037a.d24a (SR505)	1.0.38-112.70	5.100.138.2001.cpe4.12L04.3	6/5/2013
2.4.4.4	A2pD035j.d24a (SR350) A2pv6C035j.d24a (SR500)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	11/12/2012
2.4.4.3	A2pD035j.d24a (SR350) A2pv6C035j.d24a (SR500)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	10/11/2012
2.4.4.2	A2pD035j.d24a (SR350) A2pv6C035j.d24a (SR500)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	7/30/2012
2.4.3.7	A2pD030n.d23c (SR350) A2pv6C032a.d23c (SR500)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	5/31/2012
2.4.3.6	A2pD030n.d23c (SR350) A2pv6C032a.d23c (SR500)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	4/26/2012

New Features

Ref #	Description	Notes
RB-201	Wild card support for DHCP Vendor ID	
RB-264	SR350N/NE single image	
RB-375	Generate WPA keypassphrase from MAC Address	

Changes and Fixes

Ref #	Description	Notes
RB-52	LAN DHCP Server Menu Disappears	
RB-53	DHCP Server is Enabled in conf file but disabled in GUI	
RB-63	Ethernet Port configuration is missing from the GUI	
RB-87	IGMP Multicast traffic is not received from all subscribed groups	
RB-88	Wifi config is applied multiple times in 4.12.04 SDK	
RB-91	Invalid IP Address has been accepted as Radius Server	
RB-93	SR505N:LAN services are accessible when LAN FW disabled	
RB-96	Vendor ID with Amino STB	

RB-121	Policy Routing Function is not working	
RB-144	In Bridge mode, LAN Client is not obtaining WAN IP.	
RB-179	GUI buttons labeled differently and placed differently	
RB-189	no cap on number of PortMapping objects added by UPnP	
RB-190	Make default SSID configurable	
RB-209	Add TR-098 WAN DSL Diagnostic support	
RB-211	On enabling the LAN side Firewall, LAN Client is not Obtaining IP	
RB-213	SR500NE WAN will not train with 100BaseTX cable	
RB-220	MAC Address of WAN Interface created manually differs from system base MAC	
RB-225	Calix IPTV packet drops on SR500	
RB-234	STUN failure: 1. fallback period is too long 2. shutdown on incomplete state information	
RB-243	Add DHCP Relay Support	
RB-253	TR69C: Passive notification of value changes does not increment Event count	
RB-257	Enable UPnP by default for all targets	
RB-259	CPE doesn't try to obtain WAN IP on Dis-connecting and Re-Connecting DSLAM OUT Cable	
RB-262	display ADSL PTM mode option in web UI for all SRG models	
RB-263	- Calix: Non-conforming reporting on IGD.WANDe...WANDSLInterfaceConfig.DownstreamMaxRate and IGD.WANDe...WANDSLInterfaceConfig.UpstreamMaxRate	
RB-265	disable ADSL PTM mode by default in 350N	
RB-269	Memory Leak on XTM Status page	
RB-271	UPnP patch needs to be applied to 4.12-08 and earlier SDK's.	
RB-286	Add Save Default Page	
RB-291	On CnS, WAN IP is not obtained in IPoE Wan Service.	
RB-294	Display Configuration File Origin on Device Info page	
RB-309	Enable multicast packet acceleration	
RB-313	Modems will not set into "Default" mode	
RB-322	Time Zone offset being set under Automatically sync with Internet Time Servers setting is corrupting POSIX format of parameter LocalTimeZoneName for modems users using Time Blocking	
RB-323	Add configuration to force use of Base MAC Address on WAN Connections	
RB-338	Default Wireless SSID doesn't contain last four digit of MAC	
RB-342	Static Routing - Dynamically Assign Default Gateway to route	
RB-368	QoS UI bug: MAC Address mask	
RB-373	Issues during creating and editing the WAN Service	
RB-377	Firefox and IE presenting "400 Bad request" error	
RB-379	device crash on PPP auth failure with ETH WAN	
RB-381	Hide DSL Profile 30a on all VDSL2 modems	
RB-385	Static Route Remove button is misplaced in Metric field	

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.

This 2.4.4.2 FW release is the first upgrade from Broadcom 4.06 to 4.12 SDK (software development kit). The image containing “CFE” in the file name should be used when upgrading from or downgrading to pre-4.06 versions. The Broadcom version can be determined by looking at the software version in the modem’s device info page. For example this is a 4.12 version; ‘2.4.4.2_4.12L.04.A2pD035j.d24a’. Target download protection has been enabled which prevents downloads of incompatible files.

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 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 with minimal interleave delay. Sync rate increases from 2 to 4Mbps have been reported in addition to the line being more robust and resistant to noise/interference generated from treadmills, ceiling fans, etc. PhyR is disabled by default but can be enabled in the DSL menu.

Wireless is enabled by default with SSID = SmartRGxxxx (x = last four characters of base MAC). Wireless security is Mixed WPA2/WPA-PSK, passphrase = OneCpeToRuleThemAll, 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