Software Release Notes

Release 2.4.2.9

Relevant to SR Series Model(s):

SR10 ***SR100***

SR100G ***SR300N***

SR300NE

Document History

Version	Date	Author	Description
1.0	08/08/2012	M. Solomon	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 Version	DSP/xDSL Line Driver	CFE Version	Wireless Driver	Release Date
2.4.2.9	A2pB026.d22j	1.0.37-104.9	5.10.146.0cpe4.404	3/18/2013
2.4.2.8	A2pB026.d22j	1.0.37-104.9	5.10.146.0cpe4.404	1/28/2013
2.4.2.7	A2pB026.d22j	1.0.37-104.9	5.10.146.0cpe4.404	8/6/2012
2.4.2.6	A2pB026.d22j	1.0.37-104.9	5.10.146.0cpe4.404	1/11/2012

New Features

New Features		
Ref#	Description	Notes
RB-257	UPNP enabled by default.	
RB-294	Configuration file origin displayed on Device Info.	

Changes & Fixes

Changes & Fixes		
Ref#	Description	Notes
RB-52	LAN DHCP Server Menu Disappears	
RB-263	Reporting of IGD.WANDe...WANDSLInterfaceConfig.UpstreamMaxRate and Downstream corrected.	
RB-269	Memory Leak on XTM Status page corrected.	
RB-271	UPnP security patch.	
RB-287	Port Trigger addition fail on SR300NE corrected.	

Known Issues

Known Issues		
Ref#	Description	Notes
RB-23	Time blocking - browser redirect to block page may not work	
RB-28	Can't Disable DNS Proxy	

Compatibility/System Notes

Target download protection has been enabled which prevents downloads of incompatible image 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.

MAC address considerations – the source MAC address contained in upstream data equals the base MAC address. The second WAN interface uses the base MAC address plus 4 (counted in hex). Additional WAN interfaces will increment by one. TR-069 will report the base MAC address in the CWMP protocol.

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 SW Releases

2.4.2.8		
Ref#	**Description**	**Notes**
RB-36	Default PPP Authentication Retry Limit set to 65535 (Infinite)	
RB-91	RADIUS server IP field accepted invalid IP address. This has been corrected.	
RB-168	LAN side firewall was not activating on startup.	
RB-176	Add PPP Authentication Retry to PPP connections created by CnS.	
RB-234	STUN failed if connection to STUN Server was lost. STUN would sometimes exit on startup. STUN retry wait period was too long.	
RB-243	DHCP Relay support added.	

2.4.2.7		
Ref#	**Description**	**Notes**
RB-14	Number of PPPoE retries on authentication error is now configurable	
RB-11	Resolved device not retrying PPPoE authentication after error	
RB-29	Resolved Primary DNS failure not triggering switch to Secondary	
RB-31	Resolved SSID not containing last 4 characters of MAC	
RB-9	Changed SSID: "ClearAccessxxxx" to "SmartRGxxxx" where xxxx is last 4 digits of MAC	
RB-9	Changed Default WEP Key from "ClearAccessWA" to "SmartRGWireless"	

2.4.2.6		
Ref#	**Description**	**Notes**
SD-3328	Resolved incorrect LAN device status	

SW Upgrade Procedure

Upgrade Software	
Step	Description
1.0	Open a web browser, connect to 192.168.1.1/admin, and login with username **admin** and password **admin** (or appropriate IP address and login info)
2.0	Click Management→Update Software and select the Browse button
3.0	Locate and select the appropriate software image
4.0	Select the Update Software button. The software image will be uploaded to the device and the device will reboot automatically upon completion
Verify	
Step	Description
1.0	Hit the F5 Key to refresh your browser and reconnect to 192.168.1.1/admin to log back into the device
2.0	Click on Device Info
3.0	Verify the correct code is shown in the *Software Version* field

Restore Defaults	
Step	Description
1.0	Hit the F5 Key to refresh your browser and reconnect to 192.168.1.1/admin to log back into the modem
2.0	Click on the Management Link
2.1	Click on Settings
2.2	Click on Restore Default
Note:	Restoring device defaults can also be accomplished by momentarily pressing the reset button for at least seven seconds while powering on the device

Tech Support:

CPE Issues:

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

RMAs:

Open a Customer Portal ticket of type ‘RMA Request’, with title and description beginning with “RMA”, and attach a spreadsheet which includes Company Name, Model, MAC address, Issue and Firmware version tested.

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