Software Release Notes

Release 2.4.3.8

Relevant to SR Series Model(s):

SR350N   SR350NE

SR500N   SR500NE

Document History

Version	Date	Author	Description
1.0	08/15/2012	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
2.4.3.8	A2pD030n.d23c (SR350) A2pv6C032a.d23c (SR500)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.7	08/09/2012
2.4.3.7	A2pD030n.d23c (SR350) A2pv6C032a.d23c (SR500)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	05/31/2012
2.4.3.6	A2pD030n.d23c (SR350) A2pv6C032a.d23c (SR500)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	04/26/2012

New Features

New Features		
Ref#	Description	Notes
n/a		

Changes & Fixes

Changes & Fixes		
Ref#	Description	Notes
RB-4	Resolved issue with Add Port-Forward script	relevant to CV 2.3 users only
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-36	Changed default PPP auth retry max from 128 to 65535	
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"	

Known Issues

Known Issues		
Ref#	Description	Notes
n/a		

Compatibility/System Notes

This release is backwards compatible with all versions listed in the SW revision summary above. 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 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

2.4.3.7		
Ref#	Description	Notes
	Resolved issue where DNS resolution could take up to 4 seconds	
	Allow SIP ALG enable/disable from GUI	

2.4.3.6		
Ref#	Description	Notes
	Fixed a DNS Proxy issue where some sites such as www.cisco.com couldn't be resolved	
	Resolved wireless bandwidth selection not being retained after a Save	
	Resolved losing WAN access after enabling DMZ	
	Resolved Internet LED not flashing when data is present	
	Resolved daylight savings time feature not working properly	
	Resolved issue with local GUI locking up if STUN was enabled but there was no WAN connection	
	Resolved issue where editing IPoE Wan Service was not redirecting to "WAN IP Settings" page, instead it was redirecting to the "NAT Settings" page	
	Resolved an intermittent issue where if the WPA key was configured on the CPE GUI prior to checking into the ACS the ACS might corrupt the key after initiation	
	Resolved issue where the CPE was still reporting the existence of a Wi-Fi client to the ACS long after it was disconnected	
	Resolved Content Filtering configuration not being updated after a Save	
	Resolved Content Filtering not blocking any configured URLs	
	Resolved MAC address parameter not being populated for any WAN interface	
	Resolved CPE reflecting incorrect LAN ports in the Interface Grouping menu	

SW Upgrade Procedure

Which file to choose - File System Kernel or Complete Image:
Normally the File System Kernel is used unless the CFE has changed between firmware versions. Refer to the CFE column in software revision history above. The primary difference between the File System Kernel and Complete Image is the Complete Image contains the "CFE" (Common Firmware Environment, aka boot loader) which is required only when the CFE version differs

between firmware revs. It's good practice to avoid unnecessary upgrades of the CFE since a loss of power during the upgrade will result in the device becoming unresponsive.

Backwards compatibility - If there's a need to downgrade to a previous CFE version, the device's configuration may get erased during the process. A default to factory settings is recommended after the downgrade to ensure the configuration is not corrupted.

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 double click on 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 device
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 holding 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 with description "RMA" and attach a spreadsheet which includes Model, MAC address, Issue and Firmware version tested with

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