Software Release Notes

Release 2.4.4.2

Relevant to SR Series Model(s):

SR350N   SR350NE

SR500N   SR500NE

Document History

Version	Date	Author	Description
1.0	08/05/2012	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
2.4.4.2	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

New Features		
Ref#	Description	Notes
RB-3	Port Mirroring	

Changes & Fixes

Changes & Fixes		
Ref#	Description	Notes
RB-29	Resolved Primary DNS failure not triggering switch to Secondary	
RB-4	Resolved issue with Add Port Forward script	
RB-11	Number of PPPoE retries on authentication error is now configurable	
RB-11	Resolved device not retrying PPPoE authentication after error	
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"	
RB-33	Resolved changing the LAN IP address range to other than the default resulting in a failure of Content Filtering and Time Blocking	

Known Issues

Known Issues		
Ref#	Description	Notes
RB-21	Can't enable 40MHz in Wireless Advanced menu	
RB-23	Time blocking - browser redirect to block page may not work	
RB-28	Can't Disable DNS Proxy	

Compatibility/System Notes

This FW release is the first upgrade from Broadcom 4.06 to 4.12 SDK (system 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.

Port Mirroring - is a troubleshooting/debugging aid which makes it possible to monitor DSL WAN traffic from the LAN using Wireshark or other tools (only DSL WAN is supported). This feature is accessed at 192.168.1.1/admin/engdebug.cmd. For more information on using this feature contact your SmartRG rep.

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

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