1 Revision Control

Revision Number	Date of Issue:	Reason for Change
Version 1.0	February 15, 2016	Initial Release
Version 1.1	April 12, 2016	Adding rebranding CR and complete list of images
Version 1.2	July 20, 2016	Addressing several issues

2 Introduction

This document describes the new software release for Technicolor DOCSIS 3.0 modem products. These products are capable of providing up to 16 downstream channels and 4 upstream channels of traffic, depending on the hardware model. For complete details on the product specifications contact your Technicolor Sales Representative or visit www.technicolor.com.

Software changes result from feature requests and bug fixes. For each change a description of the changes is provided along with information that documents the reason for the change. If the reason for the change is to fix a problem with a previous release, a description of the previous problem is included.

This software is based on the silicon vendor's BFC5.5.9mp3CxC3.9.21.15mp3 release. This release supports new product introductions. This document is to be used by cable operators in addition to relevant models user and Installation and Operations guides.

3 Scope

This document describes changes for the following DOCSIS 3.0 modem products.

The appropriate software image should be used based on customer requirements.

4 Supported Products

Model Number	Image Name
EPC3925	e3925-E15-12-c1100r5593-160720c
EPC3928	e3928-E15-5-c3100r5593-160720c
EPC3928AD	e3928A-E15-5-c3110r5593-160720c
EPC3200	e3200-E15-5-c1000r5593-160720c
EPC3010/3008	e3000-c1000r5593-160720c
DPC3928CS	d3928-P15-5-c3100r5593-160720a

* Currently supported for demo/lab testing only until product reaches FCS status. Newer software releases may be required prior to deployment.

5 Private MIB definition files supported

SA-CM-160720.mib
SA-HW-160720.mib
SA-MTA-160720.mib
SA-Battery-160720.mib
SA-MTA-STAT-160720.mib
SA-CM-MTA-160720.mib
SA-RG-160720.mib
SA-TR069-160720.mib
SA-MOCA-160720.mib

6 Resolved issues – 160720

Item	Issue Description
1.	**(26678) The lowest frequency DS channel cannot be locked when DS load balance is enabled** Using standard 8-ch rcp-id which has only 1 receive module (instead of the real 2 modules). This setup has a bug which is now patched, when all of the followings meet: - DS load balance (downstream only in our case) is enabled on CMTS - the primary DS channel is in the 4-ch block having higher frequency range than the other channels in the other 4-ch block - the primary DS channel is not the first (lowest frequency) in its 4-ch block
2.	**(26679) Modem crash due to uncleaned Reverse Entries** When RIP is enable and a lot of connections (e.g. portscan) are built to the gateway of the RIP setup, there would be a lot of NAT session entries occupied the reverse entries in SessionTrack table, then the memory goes too low and device could crash.
3.	**(26681) WebUI: Replace Cisco Logo with Technicolor Logo and add Technicolor Copyright statement** Added support for Technicolor Branding in the WebUI

4.	**(26732) CPE is not getting DHCP IP when modem is in bridge mode** Fixed an issue where a crash is caused by reconfiguring the wifi driver when the Guest network is enabled under bridge mode.
5.	**(26921) Cannot change LAN IPv4 address from GUI** Issue fixed where it was not possible to change the 'Local IP Address' when using certain saCmWebAccess configuration settings in the config file
6.	**(26374) Faulty DTMF transmission with RFC2833** In case of DTMF transmission in conversation state with RFC2833 the DTMF signals with the signal duration of 40 ms and pause duration of 40 ms can't be transmitted correctly. The signal duration of the reproduced DTMF series can be 20 ms, 30 ms, 35 ms, 40 ms or 54 ms, that can be too short. It can cause false detection at the far-end side. (The pause duration of the reproduced DTMF series is in the range of 49 ms and 51 ms.) In order to fulfil the criteria of the correct DTMF detection at the far-end side (i.e. signal duration is min. 40 ms, pause duration is min. 40 ms) the signal and pause duration of the incoming DTMF series shall be at least 50 ms / 50 ms. Implement new patch to solve previous issue : (25293)
7.	**(26923) SSID for SoftGRE SPWIFI not being advertised** Implementing new patch for (26670) in order to fix this issue
8.	**(26924) No IPv6 address to LAN user in Dual Stack** Issue is fixed by implementing an additional reboot when switching from IPv4 RG mode to Dual-Stack mode (TLV-202=3)
9.	**(26944) Entries for wifi interfaces no longer exist in ifmib** When once switched to Dual Stack ifmib entries were generated in a wrong way for the device.
10.	**(26955) Reading of docsIfDownChannelPower from EPC3008 is 1 second longer then on other devices.** Modified call routine used for this process so it's optimized for faster performance.
11.	**(26981) Connection lost issue when RIP and extra subnet are enabled** Implemented patch from chip vendor to fix issue where packet loss could occur when device is configured in a RIP environment.

12.	**(27012) XSS possible in wlanScanPopup.asp** There is a flaw located in /wlanScanPopup.asp and allows remote attacker to inject arbitrary JavaScript code (and HTML code) and perform almost every administrative operation (like changing password, login, DNS, etc.) in web frontend without victim's knowledge. The attack vector is a specially crafted SSID of attacker's wireless network. To succeed, attacker must trick the victim to login to modem's web interface, open "Radio Settings" tab and then click "Scan APs" button. Attacker does not require any authentication.
13.	**(267013) Anti-CSRF token implementation.** Implementation of a token based anti-CSRF solution which make the request unpredictable for an attacker by including a random value that changes regularly inside HTML forms.
14.	**(26844/27017) Issue switching to mode using TLV202** Fixed an issue where it was not possible to switch the device in IPv6 by using the TLV-202= 3 in configuration file, when the device was once switched to Bridge mode using the webGUI. Issue is also fixed when trying to switch to bridge mode when TLV202 is set.

7 Resolved issues – 160215

Item	Issue Description
15.	**(26344) VRF are not working with epc3208** Fixing an issue with DstMacAddress LLCPacketClassifier causing wrong behaviour.
16.	**(26410) IP fragment packets in wrong Service flow** Solving issue CM is putting the main IP Packet in the correct Service Flow, but the remaining fragments in the wrong Service Flow.
17.	**(26612) Cisco Wireless Residential Boot Loader Denial of Service Vulnerability.** Fixing vulnerability where In early booting process, it is possible to access some administrator functions, as config file was not yet fully loaded. Cisco [PSIRT]-CSCux24948
18.	**(26615) CSCux24935 - Cisco Wireless Residential Gateway Stored XSS and CSRF Vulnerability** Fixing vulnerability reported by Cisco [PSIRT] - CSCux24935 A vulnerability in the HTTP Web based management interface of the Cisco EPC 3928 Wireless Residential Gateway could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of the affected system. The vulnerability is due to insufficient input validation of a user-supplied value and lack of encoding user-supplied data. An attacker could exploit this vulnerability by convincing a user to click on a malicious link.

19.	**(26616) CSCux24938- Cisco Wireless Residential Gateway Reflective XSS and DoS Vulnerability** Fixing vulnerability reported by Cisco [PSIRT] - CSCux24938. A vulnerability in using the web interface to configure a list of client MAC addresses on the Cisco Wireless Residential Gateway products could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to the device unexpectedly rebooting. The vulnerability is due to lack of proper input validation when a list of client MAC addresses is configured remotely. An attacker could exploit this vulnerability by sending a HTTP request with a crafted payload of MAC addresses. An exploit could allow the attacker to cause a DoS condition due to the device unexpectedly reloading.
20.	**(26617) CSCux24941- Cisco Wireless Residential Unauthorized Command Vulnerability** Fixing vulnerability reported by Cisco [PSIRT] - CSCux24941. Remote, unauthorized access to administrator functions. It is possible to use admin functions (user 'admin') from 'Status' tab.
21.	**(26670) Guest network parameters not stored in nonvol.** After modem reboot, the configuration change made by the user via the webgui for guest networks are not saved and replace with initial config file parameters.

8 New Features – 151110

Item	Issue Description
1.	**(26362) Merge PHP Client 6.0.0.2** New TR69 has been merged. Features fixed: **Description**: Reboot RPC call fails for Cable Modem builds. **Issue**: Fixed check for CmDocsisCtlThread singleton.

9 Resolved issues - 151110

Item	Issue Description

22.	**(26124) WMM enable/disable MAY NOT affect wireless throughput when IP ToS=1** Update Wifi driver to solve issue when Wifi throughput drops down when IP Tos=1
23.	**(26383) [TR-69] Modem will crash when it is set to bridge mode** Upgrade to PHP6.0.0.5 to avoid crash when the ACS sets the modem to bridge mode.
24.	**(26420) Modem crashes when check box "Show key" is selected** On the quick setup page, the check box "Show key" is unexpectedly available when saRgDot11OperMode is 2. This is causing the modem to crash when its state is modified. Issue solved by greying out the check box.
25.	**(26481) 5G can't be changed to Enable on WRadioSettings.asp** Fixing issue where If set saRgDot11BssEnable.112 to disable(2), 5G can't be changed to Enable on WRadioSettings.asp.
26.	**(26499) The buttons of QoS.asp should be displayed properly.** Fixing issue where buttons on wireless QoS page are not displayed correctly when WMM is disabled.

10 New Features – 150429

Item	Issue Description
27.	**(25918) Merge PHP Client 5.2.2.3** New TR69 has been merged. Features fixed: WiFi password can be pulled from ACS InternetGatewayDevice.DeviceInfo.X_CLEARACCESS_COM_PBCAVersion reports new version Content Filtering LAN Hosts Port Forwarding Time Blocking

28.	**(25769) Support L2GRE images for 3383, non linux platforms.** L2GRE images are now available for all 3383 non-application images such as the EPC3928S.

11 Resolved Issues – 150723

Item	Issue Description
1.	**(25897) Spectrum analyzer pages not working** When accessing the spectrum analyzer using HTTPS, the pages no longer throw a "Server unexpectedly closed the connection" error. When accessing the spectrum analyzer at the CM IP on port 8080, corrupted SA pages are no longer seen.
2.	**(25975) Modem is not sending SNMP trap to correct IP address configured in the MTA config file** Modem will no longer send traps to 68.114.37.198 rather than the configured IP address.
3.	**(26003) DPC3008 Cannot Handle Large SNMP Response Message** The modem now supports multivarbind snmpget requests. These requests can support a 54 character length sysDescr in a single PDU.
4.	**(26042) IPTV traffic does not start if IGMPV2 is used on LAN side** Yearly IPTV traffic will no longer fail to start when IGMPv2 is enabled. LAN side traffic will no longer be affected.

12 Resolved Issues – 150429

Item	Issue Description
5.	**(24446) Modem is losing fixed WiFi channel after upgrade from Auburn** Upgrading from Auburn-based images no longer changes the wireless channel set by the user.

6.	**(25069) Spoofed TCP packet causing loss of connectivity** Router no longer stops forwarding traffic after receiving a spoofed TCP packet with source and destination port 0 window size 6667.
7.	**(25583) Freeze issue when modem is in dual stack modem and HNAP is enabled** HNAP multicast using the TwonkyMedia server no longer causes the device to hang when in IPv4+IPv6 dual stack mode.
8.	**(25619) FTP Speedtest with CM-IPv6 address** FTP speed test works when using an EPC3212 provisioned via IPv6. “Socket error” debug message no longer occurs.
9.	**(25635) Voice attenuation levels are not set according to Hungary country code** The attenuation of is now correct: 3dB in sending direction 10 dB in receiving direction
10.	**(25764) Apply the WiFi country code based on CSP 901448** The German WiFi country code is now set properly to: CC: DE (E0/56) GERMANY Ver: 6.30.163.39.559.87.12
11.	**(25829) Memory leak in NATP NO-MATCH RX process** A memory leak no longer occurs after downloading multiple torrent files on hosts that had been pre-assigned DHCP IP addresses.
12.	**(25835) Slow wifi and crash** Wireless network does not crash when UPnP is enabled on NAS while running BitTorrent traffic.
13.	**(25843) saRgDot11ApsScan MIB can't be polled in bridge mode** saRgDot11ApsScan MIB tree can be read and set when saRgIpMgmtLanMode.32 has been set to Bridge.

14.	**(25926) VRF to LAN port mapping** LAN switchport can now be mapped to a desired VRF or service flow. Traffic for all ports is no longer unconfigurably set to pass through the default service flow.

13 New Features – 150216

Item	Issue Description
1.	**(25149) New MIB saRgDot11ChannelSelectionPolicy to select WiFi auto channel selection policy** Mib to select WiFi Auto Channel Selection policy. Default (0): By default the number of APs and the Composite Noise Score is used to decide the best channel available to the radio. Legacy (1): Only considers number of APs. Intf (2): Only considers number of APs and interference measurement. Intfbusy (3): Considers interference and channel occupancy (including number of APs). Optimized (4): Considers interference (including back ground noise), channel occupancy (including number of APs) and Tx power. This parameter is stored in non-vol and set to default (0) after a factory reset.

2.	**(25326) Enhance WiFi blacklist feature** The saRgDot11BssRejectPriSsidSta is in place to track the primary SSID CPEs and disallow them from connecting to hotspot SSID within the same CPE, preventing misuse of secondary SSID bandwidth. Drawback of this feature is that subscribers would never have the ability to use their own devices to test or activate the hotspot. To achieve this, a new MIB is implemented. When this MIB is enabled, the RG will allow CPEs to logon to the hotspot one time, after that the saRgDot11BssRejectPriSsidSta will kick in enable secondary SSID based MAC filtering. Name: saRgDot11BssRejectPriSsidStaCount Type: OBJECT-TYPE OID: 1.3.6.1.4.1.1429.79.2.2.2.1.1.18 Value list: 1: disable(0) 2: enable(1) Default values: 1: 0 (int)") **NOTE:** This MIB is only available in D3.0 products and applicable for secondary SSID in hotspot environment.
3.	**(25327) New MIBs to control minimum allowed connection speed for guest SP Wi-Fi users** With guest SP Wi-Fi users connecting to the hotspot it's important to have a feature that provide some kind of Qos for the home user. Two new MIBs have been implemented to control this feature : saRgWifiHotspotConnectionSpeedMin saRgWifiHotspotConnectionSpeedTimeout

14 Resolved Issues – 150216

Item	Issue Description
1.	**(24513) Time of Day rules do not work on 5 GHz band** Access Restrictions > Time of Day Rules only apply to wired connections and wireless devices connected to 2,4GHz radio. Devices are not blocked on 5 GHz radio.

2.	**(24656) ARP request send by RG LAN for entire .32 range** The modem is arping for the LAN ip addresses in the .32 network that are not in use (and have never been in use) every 10 seconds. When the modem has arped for the entire local subnet, it happily starts all over again.
3.	**(24952) Modem often stops data forwarding and WiFi clients are disconnected** This issue happens sometimes when a PC tries to connect to CM via Wifi while router is sending IPV6 router advertisement or neighbor solicitation packet. CM will lose traffic and Wifi clients will be disconnected. This issue only happens if CM is provisioned with IPV6 address or dual stack IPV4/IPV6.
4.	**(25146) CPE Inactivity timeout does not work in a certain scenario** If a smart phone is connected to the hotspot SSID and then it is moved away from the WiFi coverage area, in that case MAC address of this smart phone is never cleared from WiFi association list unless the modem or WiFi driver is rebooted. This issue prevents the new WiFi clients from connecting to the Hotspot SSID if the maximum number permitted hotspot clients are reached.
5.	**(25113) Proper switching of the unit between AC mains power and battery** For battery backed units correct switching between AC mains power and battery is implemented.
6.	**(25114) Battery thermal sensor is not enable** In previous software battery thermal sensor is not enable. With this fix thermal sensor is now enabled by default.
7.	**(25240) TR69 Wireless parameters not correct** Three ACS related issues are fixed. 1. Some TR69 parameters are not changing accordingly when WiFi mode (2.4 or 5 GHz) is changed via Web GUI. 2. TR69 parameters keep showing 5GHz band even for single band products. **3.** Also channel bandwidth 20/40 MHz is not editable from the ACS.

8.	**(25241) TR69 Adding a second IP to the LAN from the ACS replaces the primary IP** When pushing a new LAN IP to the device, it replaces the current primary IP instead of setting up a new IP or throwing an error that it can only support one such IP. When pulling the information after pushing a second LAN IP as mentioned above, it only returns information on the primary IP which has changed to what was pushed. Device does not support second IP on LAN. The TR98 model objects for the secondary IP. With this fix adding a second IP to the LAN from the ACS will be unsuccessful, and the primary IP will not be replaced.
9.	**(25242) TR69 Guest networks are set to enable by default** In mainline code base, the Mib saRgDot11BssEnable is a master switch of the wireless network. The WebGUI's priority is less than mib saRgDot11BssEnable. Current ACS implementation is based on WebGUI. This creates confusion if the end user has changed the Web GUI setting different than the Mib saRgDot11BssEnable. We have re-implemented TR69 code in our modem which is now based on the mib saRgDot11BssEnable.
10.	**(25245) TR69 Separate TCP and UDP port forwards with overlapping ranges are not readable or writable by ACS** Unable to pull or push existing port forwards that have overlapping port range (different protocols), even though they're allowed by local GUI. One of them will not show up in the tr-069 ACS
11.	**(25293) Faulty DTMF transmission with RFC2833** In case of DTMF transmission in conversation state with RFC2833 the DTMF signals with the signal duration of 40 ms and pause duration of 40 ms can't be transmitted correctly. The signal duration of the reproduced DTMF series can be 20 ms, 30 ms, 35 ms, 40 ms or 54 ms, that can be too short. It can cause false detection at the far-end side. (The pause duration of the reproduced DTMF series is in the range of 49 ms and 51 ms.) In order to fulfil the criteria of the correct DTMF detection at the far-end side (i.e. signal duration is min. 40 ms, pause duration is min. 40 ms) the signal and pause duration of the incoming DTMF series shall be at least 50 ms / 50 ms.

12.	**(25299) IPv6 modem failure with DCC load balancing from the CMTS** If a modem is provisioned in dualstack mode and then Load Balanced with a DCC, the modem would eventually become unresponsive on the IPv6 address; however, CPE traffic would pass successfully.
13.	**(25323) QAM Lock Lost After DBC Message Resulting In Slow Download Speeds** In certain load-balancing scenarios, QAM lock will be lost after a DBC message is received to modify the new primary channel. This issue results in some DS bonding being lost and very slow download speeds being observed due to all channels not being available.
14.	**(25325) ARP spoofing can be used to break isolation between LAN and public WiFi networks** The CM doesn’t enforce a complete segmentation between traffic originated on the LAN (both Ethernet and Wi-Fi) and traffic on the hotspot Wi-Fi networks. An attacker connected to the LAN network can break the separation between the 2 networks with a simple ARP spoofing technique. When a malicious user on the LAN generates spoofed gratuitous ARP traffic towards the CM interface which acts as the GW of the LAN, advertising itself as being an arbitrary internet IP, all the traffic on the public Wi-Fi network for the IP advertised by the attacker gets redirected towards the attacker’s machine on the LAN, instead of being bridged towards the CMTS.
15.	**(25375) TR69 Local GUI Click Through being blocked by default** "Local GUI Click Through" is a PrimeHome feature that lets a network manager visit the home device's webpages from the ACS. The frontend for this feature can be found in the PrimeHome GUI under Services -> Local GUI Click Through The click through is achieved by opening access from the webpages to the RG_ROUTER_IP:8080 The feature is not working because the MIB saCmWebAccessUserIfLevel.home-user.wan-rg is set to off (0) by default. This is to block WAN access to the webpages via the RG IP address. With this fix when clickthrough is enabled, RG_ROUTER_IP:8080 will be accessible from the WAN side even if this MIB is set to off (0). When the clickthrough expires, the access will be once again revoked.

16.	**(25374) TR69 Content Filtering enabled causes HTTP timeouts after some time** If content filtering is enabled it works but after some time all web pages get filtered effectively shutting down internet access (web browsing times out). After applying this fix content filtering should only block webpages not suitable for children. When content Filtering is enabled, these pages should instead redirect to the ACS showing a warning.
17.	**(25373) TR69 Unsetting an existing port forward on the WebUI does not delete the entry on the ACS** If an existing port forward entry is removed using WebUI, ACS still reports that the port forward entry exists.
18.	**(25371) TR69 Port forwards not properly synchronizing between ACS and WebUI** A number of issues are fixed related to synchronizing the Port Forwarding tables between a gateway's webpages and a Cisco PrimeHome TR69 ACS.
19.	**(25402) WAN blocking in GUI is not working when disable IP flood option through webaccess** When removing IP Flood detection from GUI it's not possible to change the value of Block Anonymous Internet Requests in GUI.
20.	**(25451) CSRF using goform/Docsis_system** This is a CSRF vulnerability which gives attacker possibility to log in with default credentials and control the modem. Attacker only needs to trick the victim to open malicious website.
21.	**(25450) XSS possible in wlanScanPopup.asp** There is a flaw located in /wlanScanPopup.asp and allows remote attacker to inject arbitrary Javascript code (and HTML code) and perform almost every administrative operation (like changing password, login, DNS, etc.) in web frontend without victim's knowledge. The attack vector is a specially crafted SSID of attacker's wireless network. To succeed, attacker must trick the victim to login to modem's web interface, open "Radio Settings" tab and then click "Scan APs" button. Attacker does not require any authentication.

22.	**(25484) SNR drops when docsis QAM and analog channel are neighboring** Only the BCM3380 chipset based modems are affected by analog video channels although they are not overlapping. This causes the SNR to drop to 29dB<SNR<33dB. This causes packet loss and slow internet access.
23.	**(25509) Packet loss after DBC on annex B setup** During DBC on 8 channel bonding, modem experience packet loss. It was also noticed that issue is present only on Annex B, since test image for annex A did not experience the issue.
24.	**(25358) Codec change during call results in bad voice quality** Bad voice quality is observed during a SIP call due to codec change from G729 to G711. This happens when MTA using the standard codec list with G729 as the first option but when the call is routed to the media gateway (that serves the IVR number) which just supports G711.

15 New Features - 140829

Item	Feature Description
1.	**(22860)New MIBsaRgIGMPMaxRspTime** Defined new MIBsaRgIGMPMaxRspTime to allow the operator to control the calculation of MAX RSP TIME in IGMP configurations. Calculation can be set to follow either IGMPv2 or IGMPv3 specification.
2.	**(22968) View Wi-Fi channel scan results via SNMP** Added the MIB tree saRgDot11ApsScan to allow the results of the Wi-Fi channel scan (previously accessible only in the web GUI) to be viewed via SNMP.
3.	**(23433) Implement holding tone for Hungarian country code** For the hungary2(22) country code, a holding tone has been implemented, to be played when the MTA receives the signal instruction S: L/ht.
4.	**(23266, 23504) saCmWebAccess bitmask additions** Added bitmasks under saCmWebAccessReadPages/WritePages for IP Passthrough and Storage and Sharing (USB, NAS, Media Server).

5.	**(23608) New MIBsaOorDsidOverride** Defined new MIBsaOorDsidOverride to allow deviation from the MULPI specification for faster recovery from Out of Range DSID packets.
6.	**(23963) Add option to saRgWifiHotspotInsertDhcpOptionsMask so CM MAC is added** New option added to saRgWifiHotspotInsertDhcpOptionsMask for insertion of the CM MAC address under DHCP option 82.2 for hotspot operation.
7.	**(24072) Improved 802.11ac Web GUI controls** For models with 802.11ac support, the web GUI controls for 5 GHz network mode and channel width have been updated to better describe the available configuration options.
8.	**(24144) New MIBl2ogreTcpMssClamping** Implementing the mibl2ogreTcpMssClamping to control the value of mss clamping in l2gre. By default the value is 0 (disabled).

16 Known Issues and Limitations - 140829

Item	Issue Description
1.	**(22860) Legacy CM-based Resiliency** The cable modem resiliency method (configured using saCmNarrowbandFallbackInterval / saCmResiliencyInterval) is not supported in this release. CMTS-based resiliency (partial service) is supported.
2.	**(24240) sysDescr is incorrect for DPC3208C model** For this release, the sysDescr for DPC3208C reports "Cisco DPC3208 DOCSIS 3.0 2-PORT Voice Modem". "DPC3208C" should be used in this field for the battery model. There is no issue with the non-battery version of DPC3208.

17 Resolved Issues – 140829

Item	Issue Description
1.	**(24807) Memory leak in NATP NO-MATCH RX process** Modem fails to free NAT session after expiring. This resulted in a memory leak.
2.	**(24799) DHCP server not handing IP addresses correctly** LAN DHCP server assigns DHCP IP leases to zombie state and therefore cannot distribute them.
3.	**(24803) When wireless 5G or 2.4G interface is shutdown, it must not be possible to sniff 5G or 2.4G BSSID packet** Fixed issue where BSSID packets can be sniffed even after disabling the 2.4 or 5GHz interface.

18 Resolved Issues – 140807

Item	Issue Description
4.	**(24154) IPTV traffic does not start if IGMPV2 is used on LAN side [RG]** The cable modem cannot handle IGMPv2 packets sent from the LAN if group IP 239.x.x.x is used. Therefor no multicast traffic will start.

5.	**(24467) Modem crash when dbc command is received for load balancing** During load balancing the modem crashes after receiving a DBC command to move to a new RCC-ID.
6.	**(24673) Verify DNS caching behavior in 5.5.9** The modem does not save the last used DNS IP address in non-vol memory.
7.	**(24619) Implement Broadcom fix to solve counter issue** The ifInOctets and ifOutOctets counters on the rf mac interface are providing incorrect data.
8.	**(24654) Slow wifi and crash** A memory leak is observed in the upnp process when applications such as torrent clients are running. This causes the memory utilization to increase leading the modem to a reboot.
9.	**(24694) EPC3925 freeze when connecting Huawei P6** Connecting a Huawei P6 smartphone to the modem results in a modem freeze triggered by the upnp process
10.	**(224707) Set saRgDeviceConfigIgnore default value to 2** Changing the default value of saRgDeviceConfigIgnore to 2 so the RG interface won't try to download a config file by default.

19 Resolved Issues – 140718

Item	Issue Description
1.	**(24689) DSSS actual power mismatch with target power** **Operational Impact**: Tx power mismatch with target power and actual measured Tx power **Technical Impact**: Modified the code to re-configure the PCI-e parameter (normal power setting) again during WiFi initialization, to resolve Tx power and Wi-Fi disable issue

20 Resolved Issues – 140715

Item	Issue Description
2.	**(24095) CM goes to "sreject(na) state if we enable EAE on CMTS"** **Operational Impact:** Due to the command "cablemodem privacy eae-policy ranging-enforcement" applied on CMTS the Cablemodem is not registering. **Technical Details:** If an active TEK exist due to EAE and after registration it is found that config file contained non default TEK grace time, refresh of TEK is required. TEK refresh should be initiated in BPI manager thread context as only that thread can cancel previous TEK expire timer and re-initiate it after key is renewed
3.	**(24394) DHCP server won't give LAN IP address if modem reboots before end of the lease** **Operational Impact:** We configure the LAN DHCP pool with /30 mask. If the modem reboots before the lease of the single given IP has ended, it won't be able to give the same IP another CPE. **Technical Details:** We make sure the only available IP can be distributed to any other CPE if the previous CPE is disconnected and its dhcplease has ended.
4.	**(24144) Add l2ogreTcpMssClamping to saL2oGREMIB tree** **Operational Impact:** MSS clamping value was in previous releases hardcoded. The new default value is 0 (disabled) **Technical Details:** Implementing the mibl2ogreTcpMssClamping to enable and set the value for mss clamping.
5.	**(24395) Dynamic DHCP IP addresses are also displayed in the pre-assigned DHCP IP addresses table** **Operational Impact:** The pre-asigned DHCP IP addresses table displays the mac and IP addresses of CPE that got their IP by dynamic DHCP, not pre-assigned DHCP. **Technical Details:** Removing the dynamic DHCP IPs from the pre-assigned DHCP IP table

6.	**(24398) DUT should not crash on 12 hrsBulkCall test (ACDS leak)** **Operational Impact:** Modem crashes during voice endurance test. **Technical Details:** Fixing memory leak issue.
7.	**(23855) The spectrum of the special dial tone contains several not required frequencies** **Operational Impact:** Some not required frequencies are seen with the special dial tone **Technical Details:** Removing these frequencies
8.	**(24399) Issues with German language support in webGUI** **Operational Impact:** When German language is selected, from LAN side Wireless tab is not accessible on the GUI and from CM IP address none of the tabs are accessible (only one page is accessible). **Technical Details:** Fixing issue so all pages are available from all interfaces
9.	**(24420) SSH access does not work** **Operational Impact:** We cannot SSH to the modems with 559mp3 release. The client will connect, asks for password and accept the password, but the prompt does not work. **Technical Details:** This is caused by un-initializing the GoodLoginBanner
10.	**(24434) DHCP LAN IPv6 failing after factory reset on epc3925** **Operational Impact:** LAN CPE won't get anIPv6DHCP address after a factory reset if modem is running in IPv6 or dual stack mode. It will only work if the modem is rebooted.

11.	**(24442) Implement saRgDeviceFactoryReset** **<u>Technical Details</u>:** Implementing the mibsaRgDeviceFactoryReset to only factory reset the RG or wifi settings.
12.	**(24444) Call waiting tone not according HU2 specification** **<u>Operational Impact</u>:** In case of waiting calls, the called subscriber can hear always 11 beeps of call waiting tone independently of the actual status of calling party **<u>Technical Details</u>:** Correcting call waiting according to the specs
13.	**(24530) saCmNarrowBandFallBackInterval should work correctly** **<u>Operational Impact</u>:** After setting saCmNarrowbandFallbackInterval to 60, the modem relocks to non-bonded channels
14.	**(24532) WPS status is incorrect after we switch wireless interface off/on from radio settings page** **<u>Operational Impact</u>:** After Disablingen re-enabling wireless interface and save settings in the Radio Settings page, the status of wps is shown as disabled. **<u>Technical Details</u>:** Fixing WPS status in WebGUI
15.	**(24535) Wireless 5G interface issue on network mode&interface on/off** **<u>Operational Impact</u>:** With some specific combination of 802. Modes, 2.4G or 5G beacon can be seen even when the interface is turned off

16.	**(24564) Issues with LAN DHCP server providing IP addresses** **Operational Impact:** LAN CPE receives a DHCPNAK from the modem is some cases where many CPE are connected to the LAN with mixed reserved and dynamic IPs. **Technical Details:** CM offer reserved IP to other CPE and changes lease to offering state, but CM sent NAK when CPE request that lease offered by CM without recovering lease state. Results in all leases are set to offering state and no ip can be handed out. CM should not offer reserved IP to any other CPE.
17.	**(24541) P15/P20 Loss plan issue: Measured Tx/Rx Gain doesn't match expected value** **Technical Details:** It appears on DPC3216 there is an issue with the Tx/RxGain levels when the MIBs are configured as different values (e.g. -5/-7 instead of -3/-3)
18.	**(24604)** One way voice issue when CM registered with multiple ds and legacy D2.0 upstream **Technical Details:** Added changes to change sid cluster to D2.0 type sid for non MTC mode dsa-rsp, dsc-req, and dsc-rsp events.

21 Resolved Issues – 140507

Cable Modem Component

Item	Issue Description
1.	**(23130) Integration ofnew CWMP client (5.1.3) for 559mp2 based releases.** **Requirements:** Upgrade the CWMP client in 559mp2 release (v3.1.8.31.27408) to address memory leaks and some bug fixes Issues that are addressed in the new CWMP client: 5Ghz SSID parameter is not writeable Fixed issue with setting MAC filtering entries from ACS Fixed issue so device sends BOOTSTRAP when expected Flush unsupported data model parameters Changing CR port ranges does not take effect immediately "Failed digest authentication" should be info, not error. Cannot solicit device after CR port range change
2.	**(24201) Broadcast/Multicast packets seen across private and public SSID in bridged case while operating in hotspot** **Operational Impact:** There is no isolation between primary network and bridge hotspot. IPv6 clients can communicate via their local link IPv6 address **Technical Details:** Isolate completely primary and bridge hotspot network to forbid all unicast/multicast traffic to be seen across networks
3.	**(23125) Multicast traffic is not forwarded to LAN side in mixed mode** **Operational Impact:** When a device is configured in mixed mode, ports that are configured as router are not able to receive multicast streams. **Technical Details:** Implemented patch so multicast packets are not drop in the internal switch.

4.	**(24264) softGRE does not work with single card configuration on EPC3928S** **<u>Operational Impact</u>:** Single card products are unable to setup a softGRE tunnel. **<u>Technical Details</u>:** Patch implemented so softGRE can be mapped to the correct interface in a single card product.
5.	**(24317) Hotspot2.0(Passpoint) is included again in beacons.** **<u>Operational Impact</u>:** Due to a maintenance patch the fix that disable the Passpoint in a previous software release was not working as expected anymore **<u>Technical Details</u>:** Disabled the Passpoint feature in the wireless driver as it was causing iOS7 devices to prompt for a username/password (instead of pre-shared key) when attempting to associate to the device.
6.	**(24260) Change wireless country setting for EPC3928** **<u>Operational Impact</u>:** Due to wrong settings it was not possible to select CH12/13 for the 2.4Ghz and it was possible to select DFS channels for 5Ghz **<u>Technical Details</u>:** Update wireless country settings so this is aligned for European regulations for non DFS certified products.

22 Resolved Issues - 140408

Cable Modem Component

Item	Issue Description
7.	**(20400) CM reports incorrect downstream power after long uptime** Corrected an issue affecting BCM3382 devices in which downstream power levels queried by SNMP (e.g. docsIfDownChannelPower) were observed to report invalid or unrealistic values on devices that have been online for long periods of time.
8.	**(23616) Advertisement of 16-channel RCP-ID in Registration Request** Corrected an issue in which BCM33843 devices (capable of 16 channel downstream support) did not advertise the CLAB-6M-016 RCP-ID in their registration request to the CMTS. In certain cases, the lack of this RCP-ID can be interpreted by the CMTS to indicate that the device is only capable of 8 or fewer downstream channels.
9.	**(23942)ftpLite is unable to achieve high downstream rates** Modified the TCP window scale setting used by the ftpLite tool to allow higher rates to be achieved for FTP speed tests.

Residential Gateway Component

Item	Issue Description
1.	**(21805) Support for backing up RG configuration to WAN-side TFTP server** Corrected an issue in the saRgDevConfBackupMIB implementation which was causing problems for the feature to allow RG configuration to be backed up remotely to a WAN-side TFTP server.
2.	**(22310) Parental control time of day issue** Corrected an issue in which time-based parental control rules were not being enforced correctly if the device's time zone setting is modified after TOD rules have already been created on the device.
3.	**(22350) VLAN Web GUI display issue** Corrected an issue where certain configurations on the VLAN webpage could cause the configuration table to display incorrectly.
4.	**(22646) Multicast packet drop during RG WAN renewal** Corrected an issue causing multicast packet loss corresponding to periods where the RG's WAN interface is renewing its DHCP lease.
5.	**(22653) 3383 battery model crash on AC power disconnect** Corrected an issue affecting DPC3929CAD/CMAD devices which caused a crash to occur when transitioning to battery power following AC power loss.
6.	**(22868) Fallback to saRgDeviceMode configured mode when user switches from bridge to router mode** In previous releases, if the user switches the device from bridge to router mode, the device will operate in the default mode (IPv4 only). This firmware release modifies the behavior to enforce the saRgDeviceMode configuration file setting (if present) when the device is put into router mode.
7.	**(22983) SSID Prefix modification issue** Corrected an issue affecting the saRgDot11BssPrimarySsidPrefix implementation which could cause multiple SSID prefixes to be set in cases where the operator changes the MIB setting in the configuration file.

8.	**(23121) Remove "80 MHz for 802.11ac" channel width option when N-Only mode is configured** When the user has configured the 5 GHz radio to operate in N-Only mode, the option for 80 MHz channel width will no longer be displayed (the option is not applicable for 802.11n operation which only supports up to 40 MHz channel width).
9.	**(23302) Ping Diagnostics webpage issue** Corrected an issue affecting the ping diagnostics webpage which was causing an erroneous "Request timed out" message to be displayed in some cases where the device did in fact get a successful ping response.
10.	**(23402) USB Device Shared Storage configuration in web GUI** On the Storage and Sharing – USB Setting configuration option in the web GUI, revised text to read as "Enable USB Devices to be Shared Storage via SMB" to clarify that the setting applies to SMB, but not FTP.
11.	**(23406) CM fails to complete registration on hotspot config** Corrected an issue in which the device could fail to complete registration when configured in bridge mode and the device's configuration file contains saRgWifiHotspotMIBs.
12.	**(23542) Preexisting port forwarding entries are not reported by the ACS server** Applied a CWMP client patch to resolve an issue in which any existing port forwarding entries already configured on an RG device prior to its initial registration with an ACS server were not properly communicated by the client, and therefore not displayed by the ACS server. This could cause a user on the ACS system to attempt to configure a port forward for a port or ports already in use on the device, resulting in an error.
13.	**(23561) Fixed IP entries should persist across reboots** Corrected issues with saRgIpMgmtDhcpFixedIpEntry implementation for assigning fixed IP addresses for DHCP clients, in which certain entries were observed to be cleared following a device reboot.
14.	**(23570) Device configuration backup failure on dual-band models** Corrected issues with saRgDevConfBackupMIBs affecting dual-band models in which certain settings for the second radio were not stored successfully.

15.	**(23585) Issues with German language support in web GUI** Corrected two issues in the web GUI that were present when the German language is selected, causing certain content to be inaccessible.
16.	**(23615) Disable Passpoint operation to resolve iOS7 interoperability issue** Disabled the Passpoint feature in the wireless driver as it was causing iOS7 devices to prompt for a username/password (instead of pre-shared key) when attempting to associate to the device.
17.	**(23633) Local IP address under LAN Setup tab can't be changed when certain web access settings are in place** Corrected an issue in the saCmWebAccessReadPages/saCmWebAccessWritePages implementation, in which the Local IP Address of the device couldn't be changed for certain bitmask configurations.
18.	**(23813)TR-069 boolean reporting** Corrected an issue in the CWMP client causing certain Boolean parameters to be reported incorrectly to the ACS server.
19.	**(23941) IE10/IE11 Web GUI interoperability issues** Corrected issues with certain web GUI controls not displaying correctly in Internet Explorer version 10 or higher.
20.	**(24186) Correction to the channel width labels** The channel width options have been set to "20 MHz Only" / "Auto (20 or 40 MHz)", rather than the "Standard" / "Wide" labels used in certain previous versions. The "20 or 40 MHz" is intended to communicate that the device may be required to fall back to 20 MHz operation due to 802.11 channel coexistence requirements.

MGCP Component

Item	Issue Description
1.	**(23120) DPC3929CAD fast charge current should be 290mA not 590MA** Corrected issue from previous release where the fast charge current setting for the DPC3929CAD was set incorrectly.
2.	**(23432) Hungary: Pause between call waiting tones is too long** Corrected issue affecting the hungary2 country code in which the pause between the first and second call waiting tones exceeded the specified requirement (1960 ms ± 10%).

SIP Component

Item	Issue Description
1.	**(22837) Remove “route” header from SIP REGISTER message** The “route” field has been removed from the REGISTER message as it has been observed to cause interoperability issues with certain SIP proxies, notably CS2K. This header is an optional requirement of RFC 3261.

23 Changes Merged from Previous Releases

Release 131025

New Features

Item	Feature Description
1.	**(22974) Support for US Accessibility Requirements** Web GUI changes implemented for compliance with the US Communications and Video Accessibility Act of 2010. For more information regarding Cisco Accessibility Design Requirements implemented, please consult the 131025 release notes.
2.	**(22712) MoCA function support.** **Requirements:** New products that have MoCA component in HW should be able to support MoCA functions in software as well. **Technical Details:** By default, MoCA on DPC3829M, DPC3929M, DPC3940M, can be used to connect another MoCA node with encryption disabled. Encryption can be enabled via CLI or the MIB. There is limited MIB support in the initial release. saMocaDevEnabled, saMocaDevResetNow. **NOTE:**saMocaDevEncryption related MIBs are not supported yet due to issues with encryption in MoCA driver.
3.	**(23130) Upgrade the CWMP client for 559mp2 based release.** **Requirements:** Upgrade the CWMP client in 559mp2 release (v3.1.8.31.27408) to address memory leaks and bug fixes. Major issues are addressed in the new CWMP client: Hard-coded wireless adapter instances need to be fixed Segmentation fault / crash if Get Parameter Attributes is called on a multi-object Memory leak on Get Parameter Attributes Bandwidth Monitor Leaks Memory CWMP client may not attempt to re-resolve ACS domain on retry Events accumulate if inform fails

4.	**(22787) High Power Wireless Card support** **Requirements:** DPC3829, DPC3829M, DPC3929C, DPC3929M, DPC3940, DPC3940M products now default to high power wireless country code for 4331/4360 wireless card combination.

24 Resolved Issues

Cable Modem Component

Item	Issue Description
1.	**(22897, 22916, 22917) After loading image, DUT will crash before scan downstream on 3010/3212** **Operational Impact:** 9After upgrading to newer base code, 3010/3212 would not properly come online. The devices were not operational in this state **Technical Impact:** Additional fixes were required when using a unified image on the newer base code to allow both chipsets to properly come online and be operational.
2.	**(23054) After reset to default DUT do upgrade the same CVC image again via config file** **Operational Impact:** After a factory reset, images for certain products 3829, 3929 would perform an upgrade one additional time. Previous release fixed the same issue for 3940, but it wasn't fixed for 3829/3929. **Technical Impact:** DUT will make sure that if upgrade has happened once already, it will not upgrade again.

3.	**(23227) INIT-RNG-REQ with new UCID causes Ranging Abort** **Operational Impact** An issue was observed in certain CMTS environments in which the CMTS would send the modem a ranging abort during upstream ranging, causing the CM to fail to come online. This issue was observed on CMs running v302r125573-based firmware. This CR modifies the ranging implementation to match that of previous releases, which does not trigger the ranging abort from the CMTS. **Technical Details** In the case where the CM's initial B-INIT-RNG-REQ gets a RNG-RSP from the CMTS with a new UCID, the CM will now send RNG-REQ instead of an INIT-RNG-REQ.
4.	**(23031) DUT should lock non-primary DS to complete provisioning.** **Operational Detail:** vendorDefaultDsFreqMIB didn't work when set in the configuration file. **Technical Details:** vendorDefaultDsFreqMIB worked when set via MIB and modem was reset. However, it failed to work when set in configuration file.
5.	**(23148) "typeofDevice" of sysDescr is not following Cisco sysDescr guidelines.** **Operational Detail:** sysDescr guidelines were changed in order to reflect typeOfDevice with more relevance. **Technical Details:** The typeofDevice ensures the type of the device as following based on their functionality.
6.	**(23113) Need to implement new command to show build options easily** **Operational Detail:** Implement a new command under CM/SA folder showBuildOptions for better understanding of each component in software. **Technical Details:** Each component in the software corresponds to a particular set of build options which can now be obtained build showBuildOptions under SA directory.

7.	**(23020) Software filename naming convention update.** **Operational Detail:** An issue was identified with correct component number for 33843 based products. **Technical Details:** Corrected build option number for 33843 application component.

Residential Gateway Component

Item	Issue Description
1.	**(22875) "Wireless Network 1" and "Wireless Network 2" should be displayed on the Docsis_system.asp** **Operational Impact:** Wireless Network 1 and 2 were not displayed correct on landing page and the fields were blank, though the values displayed correctly. **Technical Details:** Fixed the issue so that the field and values on the UI are displayed correctly.
2.	**(22910, 22896) During stress test, unit would suffer from memory leak and crash.** **Operational Impact:** Hours of stress test with data traffic ping over Ethernet, Wi-Fi clients would result in performance degradation over time. **Technical Impact:** Issue was identified with session tracking for NAT function within router code. Fixed by ensuring that TCP session track is updated in real time and hence tear down correctly, freeing up memory.
3.	**(23018) 3940 products with 33843 B0 chip have issues with linux booting up** **Operational Impact:** 3940 products using B0 chips would not come online and linux would not bootup properly. **Technical Details:** Software patch for the new hardware chip was required to resolve the bootup and linux
4.	**(22205) 5GHz settings are not being backed up in RG file** **Operational Impact:** For Dual-band concurrent products, many settings for 5 GHz wireless system were not being backed up to RG back-up file that a user can store on their PC. **Technical Details:** Reviewed and implemented backup of webUI fields that have been added for dual-band operation.

5.	**(23201) Column with 0 value on Port Range Forwarding page resulted in unexpected error.** **Operational Impact:** When you remove the value entered in port range forwarding page and input a 0, webUI threw an error stating that value of port must be between 1~65535. **Technical Details:** Fixed webUI error by making sure that with all 0 fields, it would clear the port forwarding entry.
6.	**(22950) Downstream and upstream ftp throughput is lower than pass criteria** **Operational Impact:** Issue was identified on DPC/EPC3940 (16x4) product variants where throughput was much lower than expected criteria. **Technical Details:** Found various VLAN snoops that touch the data path of packets when they shouldn't have for normal data traffic operation. Make sure these snoops didn't get installed which helped improved the performance. Issue was visible on 16 channel modems compared to 8 channel modems.
7.	**(22903) DUT crash after reset to default_ EPC3940AD_Waterloo.** **Operational Impact:** DUT will immediately crash after a factory reset for 33843 products. **Technical Details:** Issue was identified with bootloader. Fixing bootloader solved the issue.
8.	**(23324) RG on certain products will not get an IP address after reset button was pressed.** **Operational Impact:** On DPC3929C, DPC3929M, DPC3940, DPC3940M products, RG will not get an IP address after reset button was pressed. **Technical Details:** Issue was identified to GPIO mapping in the software. GPIO for reset button was mapped to GPIO for stand-by mode causing erratic behavior and resulting in RG not getting an IP address.

9.	**(22908) DUT must not crash when running CDRouterTR069 test cases.** **Operational Impact:** During CDRouter testing for TR69 sanity, crash was identified during "Verify GetParameterNames using empty string for top of hierarchy" **Technical Details:** Fixed CWMP client to ensure that when GetParameterNames is called, it would not crash.
10.	**(23167) For MoCA supported products, "M" should be contained in "modelNumber"** **Operational Impact:** According to Cisco System table guidelines, "M" should be included in Model Number for products that support MoCA. **Technical Details:** Fixed sysDescr issue in the code for MoCA products.
11.	**(22882) It has some error of UPnP and Guest network setting on VLAN** **Operational Impact:** When operating in VLAN mode, clients would not be able to use UPnP services and guest networks settings could not take effect. **Technical Details:** Modified VLAN operation to make sure UPnP and guest network settings take effect correctly.
12.	**(22718) saRgIpMgmtLanExtraSubnetTable should not be set to invalid address.** **Operational Impact:** saRgIpMgmtLanExtraSubnetTable, which is being used in B2B RIP scenario, could be set to invalid address. **Technical Details:** Modified MIB implementation so invalid address could not be set via the MIB.

13.	**(22939) The LEDs for Ethernet must be flash when CPE data activity.** **Operational Impact:** Issue with 33843 devices only where LEDs for Ethernet didn't flash when CPE activity was present. **Technical Details:** Fixed Ethernet switch code so that LEDs would blink when data activity for CPEs present.
14.	**(22760) Media server functionality doesn't work.** **Operational Impact:** Issue identified in compiling libraries for media server and check out with correct CVS tag. **Technical Details:** DMS would not appear in the DLNA capable clients and media scanning was not possible. Fixing the compilation issue + patches in base 5.5.9mp2 fixed the issue for Media Server.
15.	**(23124) USB flash's information cannot be showed at WEB GUI.** **Operational Impact:** Sometimes, when a USB device is inserted to application capable gateways, its information will not be visible on the webUI. **Technical Details:** Fixed HTTP form handler for USB device info page.
16.	**(23225) The wireless throughput result for products supporting 802.11ac were lower than expected.** **Operational Impact:** Products supporting 802.11ac did not perform well when operating in 11ac mode. **Technical Details:** Issue was identified with certain snoops that were affecting the throughput. Snoops, when not used for the feature that wasn't enabled, are now disabled not affecting data path.

17.	**(22818) Wi-Fi Radio 1 Network should have 2.4GHz and 5GHz not selectable on WEB GUI.** **Operational Impact:** For Dual-band concurrent devices running BCM4331 3x3 chip which is Dual-band selectable, must not allow Radio 1 Network to select between 2.4 and 5 GHz. **Technical Details:** In order to make sure that the end-user does not select its device operating in 5 GHz for both bands, disallowing 2.4 and 5 GHz selection for Wi-Fi Radio 1 Network would fix it.
18.	**(22873) Cannot set Wi-Fi interface to disable when "show key" is check.** **Operational Impact:** When “Show Key” check box is selected on the webUI, enable/disable radio buttons do not work. **Technical Details:** Modified webUI so that “Show Key” checkbox does not affect other fields on the webUI.
19.	**(22947) Wi-Fi security vulnerability** **Operational Impact:** Issue identified with 2.4 and 5 GHz password key fields, where inserting script would cause the webUI HTTP to execute the script and provide popup for the script. **Technical Details:** Make sure that special keywords for script and other HTTP codes are not interpreted for the HTTP server.
20.	**(23103) When the webpage wireless->radio setting is refreshed in webUI, it shows two Wi-Fi slots info even it is a DPC3828DS** **Operational Impact:** Issue identified with Single-band/Dual-band selectable single card products only. When “refresh” button was hit on the browser, two wireless slots are visible on the webpage temporarily before hiding the other one. **Technical Details:** Modified webUI HTTP form handler so that the webpage does not show 2nd slot information when it is not present in the product.

21.	**(23014) WebUI changes when WPS broadcast is enabled.** **Operational Impact:** When SSID broadcast is disabled, WPS IE should not be present in the Beacon Frames as well as webUI must have WPS disabled as per WPS 2.0 specification. **Technical Details:** WPS IE is not visible anymore for the SSID for which broadcast is disabled. WebUI is modified for following scenarios: - User is provided with error dialog mentioning that WPS will be disabled for the radio chosen to have broadcast disabled. - When both radios are selected to have WPS broadcast disabled, the WPSwebUI will be grayed out with Error in RED “WPS is disabled because both broadcast SSID are disabled”

MGCP Component

Item	Issue Description
1.	**(22820) Battery support for 3383 products.** **Operational Impact:** Current 3383 based products supported 2600mAh battery. This new implementation allows support for 3000mAh as well. **Technical Details:** 2600mAh and 3000mAh 2S1P are now supported.
2.	**(23021) The behavior of charge mode is not correct for g2 battery.** **Operational Impact:** Charge mode for g2 battery for 3383 based products was not correct for **Technical Details:** Issues for PQ and FC modes were fixed by providing correct discharge tables in the software.
3.	**(22711) saMtaEndPntTxGain&saMtaEndPntRxGain failed to provide correct gain.** **Operational Impact:** The gain settings as set by the MIB will not work correctly providing wrong values when measured using test equipment. **Technical Details:** Two issues were fixed - Issue#1: Fix was for all products in regards to RxGain calculation - Issue#2: Only was for 3383 products running Linux on 2nd thread of main processor. Libraries for DSP on 3383 were fixed.

SIP Component

Item	Issue Description
1.	**(22820) Battery support for 3383 products.** **Operational Impact:** Current 3383 based products supported 2600mAh battery. This new implementation allows support for 3000mAh as well. **Technical Details:** 2600mAh and 3000mAh 2S1P are now supported.
2.	**(23021) The behavior of charge mode is not correct for g2 battery.** **Operational Impact:** Charge mode for g2 battery for 3383 based products was not correct for **Technical Details:** Issues for PQ and FC modes were fixed by providing correct discharge tables in the software.
3.	**(22711) saMtaEndPntTxGain&saMtaEndPntRxGain failed to provide correct gain.** **Operational Impact:** The gain settings as set by the MIB will not work correctly providing wrong values when measured using test equipment. **Technical Details:** Two issues were fixed - Issue#1: Fix was for all products in regards to RxGain calculation - Issue#2: Only was for 3383 products running Linux on 2nd thread of main processor. Libraries for DSP on 3383 were fixed.
4.	**(22856) saEmtaSipDeviceFeaturesCallForwardingProcessedMIB in SA-EMTA-SIP.mib** **Operational Impact:** MIB was implemented in software but not part of Release Definition MIB files. Fixed Release Definition MIB files.

5.	**(23210) Memory leak on modems when MTA is configured only on SIP images.** **Operational Impact**: Issue was identified in the field where modems with MTA configured would crash after few days. **Technical Impact:** Memory leak was identified in DNS SRV code of the SIP implementation. Fixed leak and validated the patch to be working on the field modems.

Technicolor Worldwide Headquarters
1, Rue Jeanne d'Arc
92443 Issy-les-Moulineaux, France
T +33 (0)1 41 86 50 00
www.technicolor.com

Cisco Systems
Video Technology Group
1-800-722-2009 or 678-277-1120
www.cisco.com