Release Notes for RFS-7000 v4.4.0.0-034R & ADP-51x1 v2.6.0.0-0034R

Contents

1 Introduction to New Features

WiNG4.4 is a minor release that introduces the following features:

1. Polycom Certification for AP-650 & AP-7131N. We have successfully completed internal Motorola testing against the Polycom test plan for SVP certification. Expecting to have formal certification in the near future.

2. Smart RF - External Antenna support for AP-650. The administrator can now configure antenna gain for external antennas for AP650. This antenna gain is taken into account for Smart RF calculations to ensure that regulatory limits are not exceeded.

3. IPsec VPN Performance improvement – The number of simultaneous IKE negotiations have been increased from 25 to 100. This significantly reduces the time to bring up an entire network of VPN sessions between a WLAN controller and APs distributed at different sites. Note that this is the number of ***simultaneous*** sessions that is increased, not total sessions. e.g. Previously you could have 200 AAPs adopted to a RFS7000 over VPN, they would come up 25 at a time, now it is 4 times faster.

4. DTIM per BSS support has been added for AP-650 and AP-7131N. This allows network administrators to use a lower value for the Voice BSS/ WLAN to improve voice quality and a higher value on the Data BSS/ WLAN to improve battery life.

5. Customized Hotspot Voucher – allows the hotspot service provider to add their corporate brand name and logo on the voucher for guest users.

6. Email Alert Rate Control – Limits email alerts sent to the Network Administrator on encountering repeated flapping.

7. Mesh connection monitoring - The feature enables a client bridge to disconnect from its current base bridge and connect to a new base bridge with better signal strength

WiNG 4.4 also introduces support for the new MAC OUI “B4:C7:99”

In addition, WiNG 4.4 also makes updates to comply with the latest regulatory requirements (v 2.3)

2 RF Firmware Versions & Compatibility Matrix

Firmware version 4.4.0.0-034R

Access Point/Access Port	Firmware Version
AP300 (WISP)	00.02-37
Layer 3 AP300 (WISPe)	01.00-2354r
WIPS Sensor Image for AP300	4.6.0.5
AP100	02.05-00
AP4131	07.00-08
AP4131 Revert	00.00-00
AP650 Adaptive AP Image for AP-5131 (ADP image) Adaptive AP Image for AP-7131	2.2-1584R 2.6.0.0-0034R (sensor - 5.1.0.6) AP7131 v4.4.0.0-034R

Note: Please upgrade Adaptive AP51X1 to ADP image v2.6.0 to work with RFS switch release v4.4.0. Please upgrade AP7131 to v4.4 to work with RFS switch release v4.4.0.

For the prior Wi-NG releases on the RFS7000, please see compatibility matrix with Adaptive APs below:

RFS7000	AP5131 802.11 a/b/g	AP7131 802.11 a/b/g/n	AP7131N 802.11 a/b/g/n
v1.1	v2.0	N/A	N/A
v1.2	v2.1	N/A	N/A
v1.3.1	ADP v2.2.1 (Separate image)	v3.1.1 (to be used only in Adaptive AP installations)	N/A
v1.3.2	ADP v2.2.2 (Separate image)	v3.1.3 (to be used only in Adaptive AP installations)	N/A
v4.0	ADP v2.3.0 (Separate image)	v3.2.0	N/A
v4.0.1	ADP v2.3.1 (Separate image)	v3.2.1	N/A
v4.0.2	ADP v2.3.2 (Separate image)	v3.2.2	N/A
v4.1	ADP v2.4.0 (Separate image)	v4.0.1	V4.0.1
v4.2.1	ADP v2.4.1 (Separate image)	v4.0.3	V4.0.3
v4.3	ADP v2.5.0	v4.1	v4.1
v4.3.1	ADP v2.5.1	v4.1.1	v4.1.1
v4.3.2	ADP v2.5.1	v4.1.2	V4.1.2
v4.3.3	ADP v2.5.2	v4.1.3	V4.1.3
v4.3.4	ADP v2.5.3	v4.1.4/ v4.1.5	v4.1.4/ v4.1.5

3 Installation Guidelines

For accessing the Graphical User Interface (GUI) of the RFS7000 switches, the following browsers (and Java versions) are supported:

- Internet Explorer 6.0 , 7.0 and 8.0 on Windows 2000, XP (JRE 1.6.29)
- Firefox 2.0 and 3.x on Windows 2000, XP (JRE 1.6)
- Firefox 1.5 and 3.x on RedHat Linux (tested with JRE 1.4.2)

3.1 Firmware Upgrade Procedure

This section outlines the upgrade procedure to v4.4

The method described in this section uses the Command Line Interface (CLI) and GUI and the Auto-Install procedures. To log into the CLI, either SSH, Telnet or serial access can be used (whichever exists).

3.1.1 Upgrade the RFS7000 Switch

1. Copy the RFS7000-4.4.0.0-034R.img to your tftp/ftp server.
2. Use the "**upgrade ftp://<ip address of server>/<name of file>**" command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the switch. From CLI the command is "reload".

3.1.2 Upgrading Adaptive APs (i.e. AP7131 3.2.2 or higher to 4.4 or ADP5131 2.3.2 or higher to 2.5)

Note: AP-713x 4.0 is not a supported Adaptive AP firmware version

Note: If AP-7131 version is lower than 3.2.1, for upgrading AP-7131 to 4.4 customer has to first upgrade to pivot image AP-7131-3.2.1.0-012R and then to 4.4, otherwise the upgrade will not work.

If the AP7131 version is already at v3.2.2 you do not need to downgrade to 3.2.1. You can go directly to AP7131 v4.4.

The Wireless Switch can upgrade the Adaptive AP's either manually or automatically. The exception is Mesh client bridges which should always be upgraded manually first. For either procedure, please upgrade the wireless switch to the relevant firmware version and then follow the steps below:

For auto-upgrade of Adaptive APs

By default, auto-upgrade is enabled on the RFS Switch.

1. The Wireless switch has to host the file for the AP to download and upgrade. Please copy the Adaptive AP image files onto the switch using ftp/ tftp/ usb transfer.

2. Please switch to wireless mode. Then, configure the path to the Adaptive AP image file using command:

```
RFS7000(config-wireless)#ap-image apx131 <path where the image file is copied>
```

e.g. `ap-image ap7131 flash:/apn_04040000034R.bin`

Note: When Adaptive AP initiates adoption, the wireless switch pushes the details of the image to be upgraded to the Adaptive AP. The Adaptive AP downloads image from wireless switch and reinitiates adoption. This process is transparent to the user.

For a manual upgrade of the Adaptive APs

1. Please ensure that auto upgrade is disabled on the switch and all the Adaptive APs are adopted by v4.4

```
RFS7000(config-wireless)# no aap auto-upgrade enable
```

2. Manually upgrade from the switch all Mesh client bridges (ADP5131/AP7131)

```
RFS7000(config-wireless)# aap fwupdate n (where n is the ap index for your mesh client bridge)
```

3. Manually upgrade the Adaptive AP from the wireless switch by using the following command:

```
RFS7000(config-wireless)# aap fwupdate n-x (where n & x are the limits of your ap indexes)
```

The version of the upgrade APs can be verified by:

```
RFS7000(config-wireless)# show wireless ap<index of adopted aap>
```

or by browsing to Network-> AccessPort> AdoptedAp> FwVersion

AP5131s can only be upgraded via the switch from v2.1 (on the AP) onwards to the follow-on Adaptive images. AP-7131 can only be upgraded via the switch from v3.1 (on the AP) onwards.

3.2 Auto-Install Procedure

Auto Install works via the DHCP server. This requires the definition of a Motorola Vendor Class and four sub-options under option 43 namely:

- Option 186 - defines the tftp/ftp server and ftp username, password information
- Option 187 - defines the firmware path and file name
- Option 188 - defines the config path and file name
- Option 189- defines the RFS7000 ip address to where a L3 AP300 RF port or Adaptive AP will be adopted
- Option 190 - defines the cluster config path and file name.

Note that the DHCP vendor class for the RFS7000 is SymbolWS.RFS7000-4.4.0.0-034R

The individual features (config, cluster-config and image) may be enabled separately via the CLI, snmp or Applet. If a feature is disabled then it will be skipped when Auto install is triggered.

For the static case, where the URLs for the configuration and image files are not supplied by DHCP, the URLs may be specified via the CLI, snmp or Applet. The CLI may also be used to define the expected firmware image version. If the image version is not specified we will attempt to derive it from the file name, if it can not be derived from the filename then the system will simply attempt to load something other than what it is currently running.

Configuration files are tracked by their MD5 checksum, so if a file is renamed it will still have the same md5 sum. Once a file has been loaded it will not be reloaded, even if the local configuration information is changed.

The requested image file version, if any, is checked against the current version before any attempt is made to load it. If the requested version is the same as the running version then no further action is taken. If the image file version, embedded in the file header, does not match the expected version then no further action will be taken. If the version has not been specified then the header of the image file will be compared to the local version, if they are the same then no further action will be taken.

Please note that once the system has been operating for ten minutes, Auto Install is disabled, though it may still be reconfigured. This is to prevent the system from attempting to re-install each time a DHCP lease is renewed.

Configuring Auto Install via the CLI

There are three compulsory and four optional configuration parameters.

The compulsory parameters are:

- configuration upgrade enable
- cluster configuration upgrade enable
- image upgrade enable

Optional (only for the static case):

- configuration file URL
- cluster configuration file URL
- image file URL
- expected image version

The three enables default to yes, the URLs and the version default to "" (blank)

```
RFS7000(config)#show autoinstall

feature    enabled      URL

config       yes         --not-set--

cluster cfg  yes         --not-set--

image        yes         --not-set--

expected image version  --not-set--
```

The three enables and the expected version affect any mode of operation; the URLs are only used for the static (non DHCP option) mode.

Enables are set using the **autoinstall <feature>** command:

```
RFS7000>enable
RFS7000#conf t
RFS7000(config)#autoinstall image
RFS7000(config)#autoinstall config
RFS7000(config)#autoinstall cluster-config
```

After this configuration, any switch reboot with DHCP enabled on the port will trigger Auto Install, provided the DHCP Server is configured with appropriate options.

After the reboot switch would try to acquire the IP address from DHCP server. The DHCP server will provide the auto-install parameters like image, config and cluster-config files and paths provided if they were configured in DHCP server. Based on the parameters switch downloads the corresponding files from the specified server and reboots the box again in order to take effect the newly downloaded configurations. After the switch auto-reboot, the config and cluster-config (whichever) downloaded as part of auto-install will be applied to the switch becomes switch's running-config.

NOTE: The cluster-config will be applied to the running-config but not auto saved to the startup-config. If user wants to reboot the box again for any reason, must save the running-config using the command "write-

memory". Otherwise on the next boot, switch will have only the startup-config and not the cluster-config in running-config.

The "enables" are cleared using the **no autoinstall <feature>**

URLs and the version string are set as text and can be cleared by using an empty pair of double quotes to denote the blank string. In the following example we define the three URLs and the expected version of the image file and then enable all three features for Auto Install.

```
RFS7000(config)#autoinstall config url
ftp://ftp:ftp@192.9.200.1/RFS7000/config

RFS7000(config)#autoinstall cluster-config url
ftp://ftp:ftp@192.9.200.1/RFS7000/cluster-config

RFS7000(config)#autoinstall image url
ftp://ftp:ftp@147.11.1.11/RFS7000/images/RFS7000.img

RFS7000(config)#autoinstall image version 4.4.0.0-034R

RFS7000(config)#autoinstall config

RFS7000(config)#autoinstall cluster-config

RFS7000(config)#autoinstall image

RFS7000(config)#show autoinstall

feature    enabled      URL

config       yes        ftp://ftp:ftp@192.9.200.1/RFS7000/config

cluster cfg  yes        ftp://ftp:ftp@192.9.200.1/RFS7000/cluster-config

image        yes
ftp://ftp:ftp@147.11.1.11/RFS7000/images/RFS7000.img

expected image version  4.4.0.0-034R
```

Once again, for DHCP option based auto install the URLs will be ignored and those passed in by DHCP will not be stored.

Whenever a string is blank it is shown as **--not-set--**.

4 Important Notes

New in Wi-NG 4.4 release

1. Adaptive AP-7131 & AP-5131 now monitors the reachability to Radius for authentication. When the server becomes unreachable a SNMP trap is generated. This is configurable directly at the AP, but not at the controller.
2. Updates to comply with the latest regulatory requirements
3. May need to increase 802.11i handshake timeout in case of roaming of CB to another base bridge if there is a possibility of network delay (applicable to Mesh monitoring feature)

From previous releases

1. If you are using the IP Filtering features with ADPs, the IPfilter is not persistent on the switch when upgrading from 4.1.0.0-042R
2. The **switches in the cluster need to have a Unique/different SNMP Engine ID for Cluster-GUI** to work. After the SNMP Engine ID is changed to be unique, all switches in the cluster need to be rebooted for the change to take effect. For customers using RFMS 3.0 or MSP 2.9 with SNMP v3, you may need to rediscover your network, after changing the Engine IDs to be the same again.
3. If the user is not enabling SMART RF, but would like to share AP power and channel information across a cluster of switches, please enable through CLI "cluster master support enable". If the user is enabling SMART RF, then this CLI command is enabled automatically, the user does not need to enable it.
4. Use of SMART RF should only be enabled on AP300 & AP-5131 when using antennas with gains of 7dBi or less. For AP-7131 it should only be used with the façade antenna.
5. For the Adaptive AP, ***the Independent and Extended WLANs must be on unique VLANs***.
6. With the Adaptive AP, the number of VLANs/WLANS supported is 16.
7. Please be aware that on a hotspot authentication success page, pressing backspace on the screen restarts the time elapsed counter. However, session timeout at the back end will still remain the same.
8. In case of login issues to the applet, it is recommended to clear the java cache for the browser
9. A tagged (VLAN) port accepts only tagged packets, it does not accept untagged packets
10. It is recommended to limit Mesh networks to a single hop when managing with a switch.
11. When running a cluster of switches all switches should be running the same Wi-NG release. When using a mesh network, a single switch should be used, or if a primary-standby configuration is used. Redundancy with mesh is supported only if dynamic load balancing is disabled and only a single switch is configured in the ADP setup.
12. When TSPEC admitted units roam it is possible that the number of roamed MUs will exceed the configured max-roamed-mus count. The behavior is expected: The roaming count of MUs and air time is used only when the radio has completely exhausted the max voice air time or has max MUs associated to it which are sending voice traffic.
13. MU MAC naming is restricted to 1000 entries.
14. It is suggested that users allow a DHCP server to run on a VLAN interface even if no address range is configured in the corresponding network pool
15. When using Voice Call admission control (VCAC), please note that VCAC is disabled by default. When VCAC is enabled there are several behavioral changes, you cannot set a WLAN's QoS classification to voice, you cannot enable WLAN's voice-prioritization you cannot enable Spectra link-voice-prioritization. When VCAC is enabled, only VCAC admitted MUs get shown as voice MUs. The rest (including SVP/H323 will show as normal MUs). When VCAC is enabled, only VCAC admitted MUs traffic goes out with voice priority. The rest will be internally re-prioritized to Best Effort.
16. WLANs will have WMM enabled by default- which enables higher 11n throughput using the default setting.
17. For Adaptive AP – IP Filtering, the max number of rules per AP is 20.
18. 3G Wireless WAN is a licensed feature and the license is specific to the RFS switch and not sharable across the cluster.
19. Cluster-master-support is enabled by default for new install for WiNG 1.3 (i.e. Release 3.3 for RFS6000, Release 1.3 for RFS7000) and higher, but disabled on upgrade from pre v1.3 releases. Cluster-master support when enabled synchronizes radio information across the cluster. To disable cluster-master support use the following CLI command "no cluster-master-support enable"
20. Adaptive AP – It is recommended that you use the radius server on the switch for the independent hotspot WLAN.
21. Do not make an interface configured with a Virtual-IP a DHCP client. If the DHCP IP address gets renewed, the interface will lose all of its IP addresses, including the Virtual IP address and will be replaced with the newly acquired DHCP IP. Since virtual IP is used as a gateway IP, this will result in the clients and any other network entities in the network losing their gateway.
22. Issues have been seen with Intel 5300 11n clients running old drivers. If throughput problems are seen, please be sure to update your drivers to at least 13.0.0.107.
23. For Adaptive AP deployments with the Team Phone, please use Dynamic Chain Selection.
24. DELETED.

25. Upgrading from ADP-5131 2.4.0 to a higher version may require a reboot of the ADP-5131 before the upgrade will complete.
26. The AP650 can take up to 2 minutes to download new firmware the first time it is associated to a switch.
27. If upon upgrading to v4.2.X erroneous data is seen in the radio type fields for AP650, please close the browser and clear the java cache.
28. FTP Server on the wireless switch (pure-ftpd) can not handle more than 5 ftp sessions transferring 5 MB of data.
29. Applying serial number patch on WiNG version 4.3 will result in an error. WiNG version 4.3 supports 14 character serial numbers without the patch. The serial number patch is not required on WiNG 4.3.
30. If the serial number patch is applied to a switch with the boot partition running 4.1.x or lower and the other partition running 4.3, the patches display incorrectly on the 4.3 partition. It will display "SerialNumberUpdate (1.1)" on both the primary and secondary partitions
31. Wired Hotspot feature will work only with Layer-2 Firewall enabled.
32. DNS Whitelist
    a. Feature will work only with Layer-2 Firewall enabled.
    b. This is a CLI only feature – cannot be configured from the GUI.
33. Wired Hotspot - Traffic originated from outside network destined to a host in Hotspot enabled VLAN will not work (assuming there is a L3 router that is being used the default gateway) regardless of whether the wired host is Hotspot authenticated or not
34. Hotspot with GRE:
    a. Each vlan must be mapped to a single tunnel and the vlan id must match on the RFS switches at the two ends.
    b. Hotspot pages can be placed in remote switch across GRE tunnel and the Home switch can be pointed to use these pages as external-pages
    c. WLANs enabled for Hotspot in home switch can point to Radius server running in remote switch across GRE tunnel for authentication (similar to using external radius server for authentication)
35. LED Disable - One LED on AP-5131 cannot be disabled as it is not under software control.
36. Following is the list of storage devices tested. It is recommended that customers use one of the tested models.
    a. Flash Voyager USB drive
    b. Apache USB
    c. Cruzer USB
    d. Cruzer Titanium 2.0 GB
    e. imation USB
    f. Attache 1G USB
    g. Micro 1GB and 4GB USB
    h. iOmega [300GB] external HDD
    i. WD passport [512GB] external HDD
    j. PCIe storage: Hagiwara sys-com Express card flash memory [1GB]
    k. PCIe storage: Lexar Express card SSD [4GB]
    l. PCIe storage: Filemate SolidGO
    m. Transcend 1GB , 2GB and 4 GB USB
37. When using RFS switch with AP100 and 802.11b clients, WIDS needs to be disabled.
38. With 802.11b, upto 8 simultaneous calls with Spectralink phones are supported.
39. Live View can consume up to350 kbs(112kbs nominal) when being used in sensor/sensor mode. It can degrade the throughput over a given network link depending on available bandwidth. Networks most affected could be Mesh or 3G backhaul networks when using Live View functionality
40. During mesh firmware upgrade, client bridges get unadopted from the RFS switch prior to completion of firmware download. This does not impact upgrade which will still complete normally.

5 Issues Resolved

19231	AP-650 Installation guide has incorrect LED sequence documented for the unadopted state.
19308	Hotspot guest user fails to authenticate with the password that is modified from the GUI.
19366	In cluster mode, when '|' INC command is used, only APs that are adopted by the wireless switch which is currently logged into are displayed.

19464	The RFS6000 SYSLOG displays excessive NTPD kernel time sync error messages, even though NTP is configured properly.
19729	AP650 throughput goes down and remains around 40 Mbps when the link between PoE and wireless switch disconnected and connected back.
19756	Several AAP related commands are missing in cluster CLI.
19790	AAP Firmware update fails if the image is located in a sub-folder that contains a space in its name.
19947	AAP mesh drops and wired clients receive duplicate IP messages when proxy ARP feature is enabled.
20025	RFS7000 reboots due to the crash of CCserver process.
20054	Setting Antenna-mode on 1x1 MIMO on AP650 radio does not work. The Radio still transmits signal over multiple antennas.
20165	Dynamic-chain-sel configuration is not persistent across reboots. When dynamic-chain-sel config is enabled, it does not show up in running-config.
20175	When performing manual AP650 radio adoption, GUI requires the 802.11bgn be selected first. If 802.11an is seleced first, 802.11bgn box is grayed out.
20188	Wireless switch GUI does not display mobile device information under Security>Wireless IDS-IPS>Filtered MUs screen when DoS Association or Authentication Flood MU Threshold is met and Time to Filter is configured.
20220	E3730 HSDPA WWAN card detected as a storage device instead of modem causing WWAN card not to connect.
20266	If NAT rule is configured with VLAN <interface IP> overload, PAT does not convert the random source port from the client in the NAT translation table.
20305	Inconsistent NAS ID value (NAS-IP-Address= 0.0.0.0) being reported in RADIUS request.
20312	Applet sometimes throws Duplicate MAC error when adding APs to RTLS engine.
20468	Wireless switch does not properly report AP network mask in CLI/GUI.
20525	Wireless clients using VPN connected to AP7131 using NAT do not terminate at RFS4000.
20545	When selecting primary channel 136, secondary channel is auto set to 132 and the status message details shows - Enter proper Secondary Channel Value Invalid channel pair for the 11n radio.
20775	AP Filtering does not work when navigating pages on AP IP filter list.
20823	Sometimes hostspot users cannot login due to crash in hslogin process.
20885	AP650 does not respond to probe requests as expected in a specific scenario where one SSID name configured is substring of another SSID.
20887	The Full Release Notes for RFSX000 4.3.3 (and previous) state incorrect Driver Version for MC9090 in the Wi-Fi Certified Interoperability Devices section.
20922	Clients on the wireless network are losing connection when DHCP lease expires.
20934	Frequent reboot on both primary and standby wireless switch because of radio id mismatch and null check missing on portal config.
20936	Adaptive AP5131's running as Base Bridge reboots almost simultaneously causing the Client Bridges to lose connection. Client Bridges does not re-establish the MESH link after the BB boot up again.
20974	The radiusd process is taking up to 100% of the CPU load causing the wireless switch to crash when 200+ devices are authenticating against the internal RADIUS Server.
21160	AP650 configured in detector mode reset due to memory leak.
21196	DHCP discover and request packets do not carry option 12. The AP does not send DHCP inform packet with option 12.
21218	Hostspot failover is not working when trunking is enabled in AAP.
21320	Documentation updated - AP650 is requesting for different DNS alias than AP300.
21588	AP7131 DHCP server interface changes to static when adopted by the wireless switch 4.3.4.

6 Known Issues

New in release 4.4

There are no new issues in release 4.4 in addition to the ones listed below.

New in release 4.3:

CRID	DESCRIPTION	Resolution/Workaround
60723	Multiple Ciphers with Single SSID – When configuring through SNMP, in some cases, an invalid mapping may be accepted by the switch without returning ERROR.	In this case, the error is logged to the syslog server. Please check syslog for more information.
65821	Switch does not complain if a PoE command is issued on the tunnel interface.	This is invalid as the tunnel interface is a virtual interface.
65881	If a tunnel interface is deleted and recreated multiple times, it may not come up.	Reload the switch.
68188	Incorrect display - ADP5131 not increasing power for Coverage-hole recovery - continues on original pwr even after update from switch.	In reality, power is being increased, however, the display is not updating to show the new power.
68216	Mesh Stats: Mesh T-Put stats displayed incorrectly on the Switch GUI.	On the CLI, the stats are displayed correctly.
68441/ 68311	SFTP:F/w upgrade when using *freeFtpd Win SFTP Server* shows fail even when firmware file transfer completes successfully from the server.	This is due to a pre-configured logon message that comes with the default server. Please disable the logon message in the server for successful operation.
65376	MSTP BPDUs are not sent over GRE tunnels.	User must ensure a loop free deployment when using tunnels.
69162	Auto-upgrade via SFTP is not supported for deployments which have a mix of adaptive AP-71xx and AP-51xx.	In such situations, perform the auto-upgrade first for one AP type (e.g. AP-71xx and then the other one e.g. AP-51xx)
69220	With certain versions of Internet Explorer, clicking on the link to connect to the Wireless Hotspot does not work the first time	Clicking the link again or doing a refresh on the browser redirects the user to the correct login page
69590	AP-7131 power cannot be set to 23dBm when configuring through the RFS switch GUI	Use the CLI interface.
69674	Number of adopted APs is off by one no the GUI in the Security, Access Point detection, Authorized/ Ignored APs – when the Display Adopted APs check box is checked.	
WiNG00078547	Sometime user does not get "no service" page after Hotspot failover using IE 8	

From prior releases:

Known issues have been grouped by functional area. Issues that cross functional areas are listed in both sections for completeness and to aid the reader in researching an issue.

QoS, Voice & Roaming

CRID	DESCRIPTION	Resolution/Workaround
44103	UAPSD parameters are not displayed for Mobile-devices associated to an Adaptive-AP.	This is only a GUI issue, UAPSD is enabled on the back end
52572	Voice stats: Calls per radio (current) does not get updated and other call stats are all wrongly displayed	Mus are initially associated as regular Mus. Only when they send any voice traffic they are identified as voice Mus so until the call is established these Mus will not show up as voice Mus. And these will be considered as voice Mus until they are reassociated and hence the current call, calls max and calls average never change until the Mus are reassociated. Correct information can be found in the CLI.

Adaptive AP

58197	AAP: A extended wlan marked for EAP-TKIP security profile mapped as the 8th wlan for a aap radio fails to associate any Mus	This problem exists on all our AP types. WLAN with no encryption and WLAN with TKIP/CCMP cannot be mapped to the same bss, as the beacons are transmitted with the leasleast common denominator and TKIP/CCMP clients do not associate to WLAN's with open encryption. Map similar WLANs to one single BSS
59270	AAP: "Error: AP do not have sufficient number of radios for this configuration" message generated erroneously when "ap <mac> radio-config all-radios-off is issued.	If radio configuration is to be changed via configuration import, the older radio configuration must be deleted.
55629	AAP: Radio Switch RF stats are incorrect in CLI, SNMP and GUI	Switch and AP7131 radio stats are different because RF stats are sent in 30 sec interval. So AP side stats are more current than the switch side.
52582	AAP: After importing config file to an AAP (NOT from the RFS switch), the portal does not get configured.	If user imports config directly on the AAP bypassing the switch, please reset the AAP.
57172	AAP: Switch fails to adopt WIPS radio of AAP7132, configured in abgn wlan & sensor radio mode configuration upon reboot	Don't use two power sources on a single AP7131. Either use power injector or a PoE to power up radios. Otherwise if Power Injector goes down and PoE does not supply enough power, then some radios will go down.
57301	AAP7131: Upgrade to 3.2.1.0-012R before upgrading to 4.1.0.0	Please see the section on firmware upgrade above.
44103	UAPSD parameters are not displayed for Mobile-devices associated to an Adaptive-AP.	This is only a GUI issue, UAPSD is enabled on the back end
52892	Enabling a new WLAN causes disassociation of all Mus connected to different WLAN with Manual WLAN mapping	Changes to advertised WLANs on an AAP causes it to bring down all radios and reinitialize
45167	Hotspot configuration for Independent WLANs on an Adaptive-AP cannot be configured from the switch.	The configuration does get pushed for the extended WLAN and therefore allows for a centrally configurable and manageable hotspot.
44971	Adaptive AP cannot be adopted using the secondary IP address of a Switch Virtual Interface (VLAN interface).	Please use the primary IP address
49342	Deleted AAP radio will not be adopted after enabling	This can be recovered by doing the

	adopt unconfigured radio.	following: 1. Delete the AAP. 2. Reboot the AAP. 3. Reboot the switch.
55293	Auto-upgrade for Adaptive Aps won't work for mesh adopted Aps	When dealing with an adaptive mesh the user should manually upgrade the Aps starting at the 'outside' of the mesh (the farthest client bridges) and work their way 'in' to the base bridges. This will ensure that all Aps are upgrades correctly and no AP is orphaned in an unattached state.
54018	Enhanced Beacon Table rogue AP detector functionality does not work with Adaptive Aps	Adaptive Aps will only scan on their current active channel. Enhanced Beacon Table functionality will be supported in a future release.
53945	Rogue AP containment can be turned on for rogue Aps that are detected by Adaptive Aps (although adaptive Aps do not support AP containment).	Please do not set containment for Aps if you are using adaptive Aps. Adaptive AP containment will be supported in a future release.
53526	The SOLE engine only supports up to 256 adaptive Aps	This increase will be supported in a future release.
52802	Adaptive Aps are not always referenced by the same MAC addressed in different areas of the switch UI	The MAC address shown for adoption will be the AP's WAN/GE1 MAC address regardless of what port is connected to the switch, however the MAC addressed used for DHCP reservation will be the MAC of the interface used to connect.
55311	Channel information may not display correctly on redundant switches when using adaptive Aps	Correct channel information can be found in the primary adopted switch. Please use the primary switch for channel information.
55385	When redundancy is enabled, the wrong number of AAPs is shown adopted from switch licenses page	With redundancy enabled, the license page becomes invalid. Please look at the redundancy pages to see valid information. 1-redundancy pages show correct license information. 2-show wireless ap shows correct license information.
54118	Mobile Units not getting assigned vlan in balanced distribution when switch is configured for multiple vlans per wlan	Multiple VLAN for one WLAN feature is not supported for AAP Mus. Only Dynamic VLAN assignment using Radius is supported.
53718	Radius Accounting does not work for Mac-Authentication when using Adaptive AP	This will be addressed in a future release.
55458	Domain Name and DNS Server IP addresses are not being updated properly in Adaptive Aps	This will be addressed in a future release.
55546	AP Reset with maximum retransmission limit reached when the membership info for wireless filter changed	Pushing configuration changes to adaptive Aps with a large number of ACLs should not be done more rapidly than once a minute.
61728	Upon upgrade from 4.0.0.0 to v4.2.X the switch running config will show AirDefense WIPS radios as being in WLAN mode	

Clusters, Redundancy, Virtual IP

CRID	DESCRIPTION	Resolution/Workaround
59205	WWAN: Wireless wan Ip address is not pingable from anywhere on the internet.	ISP blocks incoming ping traffic to its assigned IP address. You can ping internal networks even though you cannot ping your

CRID	DESCRIPTION	Resolution/Workaround
		WWAN interface IP.
59261	VIP: Peer switch remains in Initialized state after fixing a configuration mismatch	Fix configuration mismatch, disable and re-enable VIP.
52592	Cluster GUI: Customer cannot edit radio configuration for AP's not adopted.	
44971	Adaptive AP cannot be adopted using the secondary IP address of a Switch Virtual Interface (VLAN interface).	Please use the primary IP address
37592	The discovered switches are lost after a reboot	Work around: If you just reload the switch and keep the browser open the dropdown box with the other switches IP will remain.
55311	Channel information may not display correctly on redundant switches when using adaptive Aps	Correct channel information can be found in the primary adopted switch. Please use the primary switch for channel information.
55385	When redundancy is enabled, the wrong number of AAPs is shown adopted from switch licenses page	With redundancy enabled, the license page becomes invalid. Please look at the redundancy pages to see valid information. 1-redundancy pages show correct license information. 2-show wireless ap shows correct license information.
62760	Active redundancy across 3 or more switches will cause ports to flip between switches in certain network topologies	Set one of the switches to be a standby
62847	For Layer 3 adoption: When more than 6 switch IP addresses are present in option 189, the AP650 will only attempt to connect to the first 6.	Please manually adopt/unadopt AP650s between the switches if necessary for full load balancing.

Security & Firewalls

CRID	Description	Resolution/ Workaround
57856	Rogue AP – ignored aps / unauthorized /authorized ap detection count is incorrect	Caption is misleading since there may be duplicate entries for the same rogue AP when detected via multiple Aps. Count is in fact correct.
59066	Ipsec: Encrypted flows do not get counted as part of Max flows per MU.	If MU has established a remote VPN tunnel to the switch in that case max flows will not count the flows established from such Mus as all the packets will be encrypted and VPN feature is not integrated with max flows per MU feature. So flows coming from the vpn gateway are not associated with an MU, and thus not counted. Only flows where the SMAC or DMAC is the MU's MAC are counted. So max flows per MU feature will not be applicable for the Mus establishing
58461	Hotspot–Logout hotspot user if browser is closed does not work for tab based browsers IE7/ Firefox.	User will be logged out after inactivity period.
56458	SPR16723: Hotspot–Logout hotspot user if browser is closed does not work with pop-up blocker enabled.	Workaround – User will get logged out (deauth) after inactivity period (idle timeout)
57360	Hotspot : Able to create guest user with start time expired	Switch does not complain if the start time is prior to current time.
57189	IDS/IPS : Configuration is not persistent when user	Default values of some parameters have

	upgrades from 4.0 ids to 4.2.X wips	been changed per the new design of the IDS/ IPS feature. (e.g. Default value for time-to-filter was 60 in 4.0 and 0 in 4.2.X; Detection window was 10 in 4.0 and 60 in 4.2.X; If you have changed values of these configuration parameters from their default values, you are advised to remove them and use the new defaults instead or pick new values – see System/ CLI Reference Guide for more details.
58816	WIPS: Disabled radio cannot be converted to sensor and vice versa via CLI.	Enable radio first.
59400	Audit Logging: No Audit logs generated for CLI commands that fail to execute.	
57268	CLI: Radius test authentication succeeds with wrong ssid.	SSID is not used by this command and can be ignored.
58986	802.11w is not supported on AP100, AP4131	
58077	Rule-descriptions will not be created if user creates a rule through applet	Use CLI interface if you want to add descriptions to the rules.
59471	Ipsec VPN : Not able to connect VPN client while using remote VPN with L2TP	. L2TP VPN connection from WinXP SP2 – Marvell 11n card and Intel 2200BG client card does not work to the Wireless Switch.
41870	Rogue AP: Duplicate entries are recorded in the Approved and unapproved AP list if two detectors detect the same AP.	
39446	Console hangs in the case of excessive static NAT entries	System is fine with up to 128 NAT entries but there is a 15 second delay
36996	Changing username/password for AP port authentication doesn't take effect immediately.	A reset or power off/on is currently required.
50187	Detector Aps may reboot when browsing through the Rogue AP report.	No network disruption, as this only affects detector mode Aps.
54791	Group Key rotation is not supported on the Adaptive AP mesh backhaul WLAN.	Do not set a key rotation interval for the backhaul WLAN. This will be supported in a future release.
53690	Adaptive Aps adopted in IPSEC mode exhibit a drop in traffic performance when large packets (over the fragmentation limit) are sent.	IPSEC adoption should be used primarily in situations in which it is necessary, otherwise normal adoption is recommended.
54018	Enhanced Beacon Table rogue AP detector functionality does not work with Adaptive Aps	Adaptive Aps will only scan on their current active channel. Enhanced Beacon Table functionality will be supported in a future release.
53945	Rogue AP containment can be turned on for rogue Aps that are detected by Adaptive Aps (although adaptive Aps do not support AP containment).	Please do not set containment for Aps if you are using adaptive Aps. Adaptive AP containment will be supported in a future release.
53760	Using "Any" option for the source or destination of a crypto ACL causes connectivity problems	It is highly recommended that the 'Any' option not be used for crypto ACLs.
52700	Client fails to associate to a WLAN that has mixed mode encryption available.	Certain clients (such as Windows Zero Config) have an issue downgrading security from CCMP to TKIP if CCMP is advertised in a mixed mode WLAN.
50834	The Role Based Firewall does not accept location as part of role configuration	This will be addressed in a future release.
52676	IGMP snooping does not check wired only traffic	This will be addressed in a future release.
55251	Network Admin unable to Disconnect an MU, add a MAC name or edit a MAC name through the GUI	Please use the CLI to perform these functions.
55621	Attacks that are detected at L3 will not be routed,	There is no communication between the L3

	but may still be bridged at L2	& L2 firewalls, this will be addressed in a future release.

General

CRID	DESCRIPTION	Resolution/Workaround
43606	User Account with a (‘) character in password causes login failure	Please refrain from using (‘) special character in the switch login password
58100	Switch management through the Applet interface would become very slow if the switch is passing very heavy bridging or routing traffic through its different ports.	Use management port on RFS6000/ 7000.
56676	SMART RF causes wsInfraCfgManageRunningCfgChangedFlag change to True causing RFMs to fail config check	Smart-rf config changes when scheduled recalibration is enabled. If calibration is scheduled and kicked off at that scheduled time, then isInfraCfgManageRunningCfgChangedFlag will be set to true.
39653	Switch console may hang for 20 minutes when large configuration file is copied to running config	When you load large configuration by copying to running-config, it may be slow. The recommended approach is to copy to startup config and reload the switch – this is much faster.
37280	Not possible to clear the DDNS IP bindings from the switch from CLI,APPLET and SNMP	The work around is that the DNS server which is managed by IT can clear the database using separate commands
40183	Network > Access Port Radios > WLAN Assignment page display incorrectly and “Index” filter not functioning	This only happens when the user is frequently switching between tabs. A refresh of the screen displays the right values.
39552	IP address in with leading zeros aaa.bbb.ccc.ddd format to a target server (to transfer a file or firmware) is not working i.e. 192.168.2.1 works but not 192.168.002.001	To be resolved in a future release
40110	Radius server restart to pick up configurations changes takes 2 minutes if 5000 radius users are present.	The config change will be picked up, but it takes 2 minutes for radius service to start itself once it had stopped to pick up the config changes. During this period any eap authentication or hotspot authentication tried will get failed.
37094	No option to enable portfast on interface from applet	Can be applied through CLI: In CLI int ge1# spanning-tree port-fast
36996	Changing username/password for AP port authentication doesn’t take effect immediately.	A reset or power off/on is currently required.
48827	USB: Drive mapping changes when an USB Flash drive is unplugged and plugged back while data transfer is in progress	Please do not unplug the USB while it is in process.
50469	Hotspot+Guest user+Applet: Not able to create Guest user when switch time is 00:00 (24hr format) from Applet	Guest user will not be created and it will display error as “switch date should be greater than current switch date”.
49356	RTLS: ‘reader 1 antenna 1 power’ doesn’t really apply to the third party reader	Please set power levels directly on the reader.
52702	Switch goes to diag mode after a reboot when the user attempts to log in. Happens most often for complex configurations.	The user should wait 2 minutes after a reboot before logging into the system to allow full configuration to be loaded.
51672	Marking on VLAN interface is not implemented	This will be supported in a future release.

CRID	DESCRIPTION	Resolution/Workaround
55365	Upon login a core file will occasionally be generated and the user will not be able to login	The Admin can simply re-attempt their login; this has no affect of the system.
54288	Hotspot access on an independent WLAN will not be limited by the Hotspot Simultaneous Users limit on the switch.	Set your hotspot WLAN to be an extended WLAN to leverage the switch's setting.
52914	'wsSwMacName' node is missing under wsSw in the SNMP tree	Workaround: There was a dependency on one SMI file and hence the SW MAC NAME MIB was not loaded. To make sure all the MIBS are compiled properly follow the below mentioned steps. 1) Batch compile all SMI files in the directory. (/path of the mibs/*SMI*.*) 2) Batch compile all SNMP files in the directory. (/path of the mibs/*SNMP*.*) 3) Batch compile all files in the directory. (/path of the mibs/*.*)
52700	Client fails to associate to a WLAN that has mixed mode encryption available.	Certain clients (such as Windows Zero Config) have an issue downgrading security from CCMP to TKIP if CCMP is advertised in a mixed mode WLAN.
55278	USB Firmware upgrade option is missing from the GUI	Please use the CLI if firmware update is being done from a USB source.
55251	Network Admin unable to Disconnect an MU, add a MAC name or edit a MAC name through the GUI	Please use the CLI to perform these functions.
55210	Hotspot users see a drop in connectivity when roaming between multiple switches in a cluster	This will be addressed in a future release.
55157, 55091	DHCP_Client ingress port displays erroneous information in certain roaming situations	This is a display issue that does not affect operation. This will be addressed in a future release.
55134	AP100 does not use RTS/CTS when a data packet exceeds the RTS threshold	This will be addressed in a future release.
51430	MAC Naming Feature cannot have special characters. ('\' '/' ':' '*' '?' '"' '<' '>' '|')	
54415	Upgrade hangs, not a watchdog timeout	In rare instances, a firmware upgrade will not complete. A ctrl-c is required to stop the upgrade session and the administrator will have to try the upgrade again.
54091	with large number of configurations, the switch goes into diag mode after reloading it	User will have to wait for a minute and try logging in again.
55430	Switch not allow to pass TCP traffic when MU associated with primary address tries to FTP MU assocated with Secondary address	This is due to the two firewalls (L2 and L3) in switch. The L3 firewall does TCP seq no randomization which causes the L2 firewall to drop the packet. This will be addressed in a future release.
54528	RFID XR400 : switch shows 4 antennas connected while only one antenna is connected	This is a problem with the LLRP implementation on the RFID-reader side. This will be considered for a future release.
55425	RADIUS logging will not roll over from primary to secondary RADIUS server if primary fails	
62220	When using the CLI:Unable to start Radius Server when group name is configured with space	Please refrain from using a space in the group name.
61918	TFTP: last timeout and gzip: can't write error seen when generating the tech-support file and passing on to the TFTP server.	

CRID	DESCRIPTION	Resolution/Workaround
60088	In a mixed environment of AP300 & AP650, the state will not change from Normal to Self-Healing when one heals for the other	
61734	The switch does not re-authenticate on behalf of HotSpot authenticated MUs when re-Auth period is set	
60556	SmartRF is done for AP650 considering only 40MHz channels, regardless of the channel width configured for the APs.	

7 A Note on Cluster UI

Once a user enables 'Cluster GUI' on the Redundancy page (under Services sash), the user will be in the cluster GUI context similar to the 'cluster-cli' context (provided the 'Enable Redundancy' option is turned on too. This context lasts until the user is logged in and will be lost every time a user logs out of the GUI (similar to what is done in the cluster cli - the context is lost when a user logs out of the switch).

If the 'Enable Redundancy' option is deselected, automatically the 'Cluster GUI' option will be disabled.

One can see the switches participating in the Cluster GUI by seeing the 'Member' tab in the 'Redundancy' page (Services -> Redundancy). The 'Status' has to show 'Established' as well against each member switch. If a 'Not Seen' is displayed against the status, then the switch will not be displayed in the cluster GUI.

Functionality supported with the Cluster UI

a. Wireless LAN(under Network sash, choose Wireless LAN and the Configuration tab)

Operations supported are:

Display: The data will be fetched from all the switches in the cluster and will be sorted based on the index value. One will see the additional Switch column to the left to distinguish data from each switch.

Note: If this page was clicked for the first time after the 'Cluster GUI enabled' checkbox was selected, then there will be a time delay until the data loads completely. This happens only for the first time since each of the Switches needs to be logged into (only for the first time). This time delay is proportional to the number of switches in the cluster times 5 seconds. It is necessary that all the switches are reachable from the current switch (If not, a message will be shown to the user saying that a particular switch is not reachable and hence data will not be fetched for it).

Configuration: On selecting a single row and clicking 'Edit', it will bring up the Edit dialog. When one edits a couple of fields in the dialog and clicks on 'Apply To Cluster', it (only the changes made) will be applied to all the switches in the cluster.

If one wants to only apply changes on this particular switch only, one can click on 'OK' button.

The sub dialogs for instance the 'Config' button against the Encryption type 'WEP 64' contains its own 'Apply to Cluster' button (this is for applying the data on the sub dialogs across the cluster).

Note: On multiple select of rows (belonging to different switches, the 'Edit' button will not be visible), however on multiple select of rows belonging to the same switch, the Edit button is enabled and the Edit dialog will display common fields that can be edited across multiple WLAN entries pertaining to the selected switch and in this case the 'Apply To Cluster' button is disabled.

Enable/ Disable option on selecting multiple rows works as before and is allowed across different switches too.

Currently, the 'Global Settings' button is not supported for cluster mode, nor are the other tabs under Wireless

LAN apart from the Configuration tab.

b. Mobile Units (under Network sash, choose Mobile Units and the Configuration tab)

Display: Same as Wireless LAN.

Configuration: Since the only editable field in this page is the MAC Name, one can edit the field on different rows belonging to different switches (one at a time) and then click on 'Apply' finally.

c. Access Port Radios (under Network sash, choose Access Port Radios and the Configuration tab)

Display: Same as Wireless LAN.

Configuration: Similar to Wireless LANs. However, since the AP Radios have different indexes on different switches, the changes applied will be seen on the corresponding AP Radio on the corresponding switches in the cluster (sharing the same MAC Name but may have different indexes - so this may appear different).

Add - One can either add an AP Radio to this switch or across multiple switches.

One can select multiple rows and click on '**Delete**' option to delete AP Radios across switches in the cluster.

Note:

The 'Global Settings' and 'Tools' button are unsupported as of now in the cluster mode.
Since the 'Group ID' belongs to a single switch, one cannot apply it on the cluster.

Other details:

On each of the first pages(in the Configuration tab for cluster supported pages), there is an option where a user can select a particular switch and see data corresponding to the selected switch or can choose 'All' to view data from all switches. One can see this option only from the first pages and. This option will not appear on subsequent pages, since paging is not supported for data fetched from a particular switch using this option.

On clicking the 'Save' button besides the Logout option; one can save the data from the running-config to the start-up config for all the switches in the cluster.

Some Known Issues:

- Sort is supported only on the data on a single page and not across the entire set of data.
- Sometimes there is a refresh problem and certain rows may appear missing, a click on 'Refresh' should solve the problem.
- It is necessary for the switches to have different Engine IDs for the cluster GUI feature to work properly. One will see issues after a reboot of any switch sharing the same engine id with another switch. In this case, data will be loaded only from one of the switches and leads to inconsistency.
- If one is using the discovery option and choosing between different switches (in the 'Connect To' option from the 'Login Details' on the left bottom corner of the main panel), then one will always see the message "Cluster GUI is being enabled" for the cluster supported pages. This will not be shown if you browse pages on the same switch thereafter.
- A maximum of 20 sessions can be open to the same switch (due to SNMP v3 security restrictions).
- Cluster GUI is not supported in a NAT'ed environment.

8 Changes to Default Values

Stateful packet inspection has been disabled by default.

9 Wi-Fi Certified Interoperability Devices

Motorola EWLAN access points are tested and can interoperate with Wi-Fi certified client devices. In addition, following is the list of clients that have been validated for interoperability with this release.

Motorola Handheld Clients

Model	OS Type	SW Version	Driver Version
PPT 8846-3717	Windows Mobile Version 4.20	3.9.3.76	3.93.79.186
PPT 8846-3717	WIN CE.NET	3.9.3.70	3.93.79.181
MC7090	Windows Mobile Version 5.0	Fusion	2.5.299.0.73B-WM Photon
MC7094	Windows Mobile Version 5.0		
MC9090	Windows Mobile 6.1 Classic	WM 6.1 AKU 1.1.5 build 19590 1.09.00	Fusion 2.57.0.0.18R PHOTON10 3.0.0.266
MC9060			
MC5040	Window Mobile	4.21.1088	3.9.2.71
MC5040	Window Mobile	4.21.1088	3.9.2.71
MC75	Window Mobile	5.2.705.21000	2.60.0.0.026R

Laptops

Model	Wireless Adapter	Driver Version	Description
Acer Travel/Mate 4500	Linksys WPC 600N V1.1	4.150.31.0	Dual Band 802.11abgn
Gateway M465	Proxim 801.11 abg8480-WD	3.0.0.104	
Toshiba Tecra A6-57B	Intel Pro/Wireless 395ABG	11.5.0.32	
Toshiba Tecra A6-57B	D-Link DWA-160	11.5.0.32	11N Dual Band USB Adapter
Toshiba Tecra A6-57B	Intel Pro/Wireless 395ABG	11.5.0.32	
HP Compaq6910P	Intel		
HP Compaq nx9008	Symbol LA-4131	3.9.78.178	
Dell Latitude D620	Linksys WPC 600N V1.1	4.150.31.0	Dual Band 802.11abgn
Dell Latitude D620	Cisco 802.11abg CB21AG	3.0.0.104	
Acer Travel/Mate 4500	Intel Pro/Wireless 2200BG		
Lenovo	Intel Pro/Wireless 2200BG		
Lenovo	Atheros AR5KXB-0092DA	7.7.0.448	Wi-Fi testbed client
Lenovo	Broadcom BCM943224HMS	5.10.112.2	Wi-Fi testbed client
Lenovo	Intel 533AN_MMWWG2	13.0.0.72	Wi-Fi testbed client
Lenovo	Ralink RT3800PD2	1.4.11.1006	Wi-Fi testbed client