Release Notes for WS5100 v3.3.1.0.0- 003R

Contents

1 Introduction

Wi-NG v1.3 is a minor feature release for Motorola's Enterprise-class RF & Wireless Switches that enables a Wireless Enterprise by delivering an extremely resilient, high performance network that ensures seamless & secure voice and data communications. WI-NG v1.3 maps to v3.3.1 on the WS5100 platform.

Key features in Wi-NG v1.3 to include:

Resilient and High Performance Networks with:

- SMART RF Management provides the capability for automatic analysis, configuration, and monitoring to optimize an ever-changing RF environment

RF Networks **securing mobility** by providing:

- Rogue AP Containment
- Ad Hoc Network Detection
- .11n Rogue AP Detection
- Detection of de-authentication from broadcast source MAC
- Detection of frames with invalid sequence number

Quality of experience and Service for VoIP users

- TSPEC Admission Control

Other system enhancements in this release include:

For the Adaptive AP 5131(ADP image v2.2.1):

- Rogue AP detection
- Mesh statistics
- WLAN statistics
- Configurable IPS Sensor on the AP5131 in Adaptive mode for the D mode SKU(ADP image v2.2.1)

With the AP300:

- Dynamic Load balancing of APs after a primary reverts in a cluster
- Email Notification for critical alarms
- Cluster GUI for WLANS and AP functionality
- Securing Layer 3 AP and Wireless Switch protocol – Secure WiSPe Protocol
- MU Naming
- IP v6 Client Support

In addition to the new features above, the following functionality have also been enhanced in this release:

LED blink pattern for locating AP300s

To locate a particular AP300 in that has been installed, the user can now make the AP300 flash its LED by using the following command:

```
"radio <index> location-led (start-flashing | stop-flashing)" commands under "wireless" context.
```

CLI command to show description fields for APs and Mobile Units

The user can customize the show command outputs for show wireless mobile-unit and show wireless radio:

```
WS5100#service wireless custom-cli ?
  sh-wi-mobile-unit  customize the output of the "show wireless mobile-unit" command
  sh-wi-radio        customize the output of the "show wireless radio" command

WS5100#service wireless custom-cli sh-wi-mobile-unit ?
  ap-locn     location of the AP where the mobile-unit is associated
  ap-name     name of the AP where the mobile-unit is associated
  channel     the channel of the radio where the mobile-unit is associated
  dot11-type  the dot11 radio type of the mobile-unit
  ip          the IP address of the mobile-unit
  last-heard  the time when a packet was last received from the mobile-unit
  mac         MAC address of mobile-unit
  radio-bss   the bssid of the radio where the mobile-unit is associated
  radio-desc  description of radio where the mobile-unit is associated
  radio-id    radio index to which the mobile-unit is associated
  ssid        the ssid of the mobile-units wlan
  state       the current state of the mobile-unit
  username    the Radius username of the user connected through this device
              (shown only if applicable and available)
  vlan        the vlan-id assigned to the mobile-unit
  wlan-desc   the wlan description the mobile-unit is using
  wlan-id     the wlan index the mobile-unit is using

WS5100#service wireless custom-cli sh-wi-radio ?
  adopt-info  adoption information about the radio (whether its on current
              switch, or some other switch in a cluster)
  ap-locn     location of the AP to which this radio belongs
  ap-mac      MAC address of AP to which the radio belongs
  ap-name     name of the AP to which this radio belongs
  bss         the bssid of the radio
  channel     the configured and current channel of the radio
  dot11-type  the dot11 type (11a/11g etc)of the radio
  num-mu      number of mobile devices associated with this radio
  power       the configured and current transmit power of the radio
  pref-id     the adoption preference id of the radio
  radio-desc  description of radio
  radio-id    radio index in configuration
  state       the current operational state of the radio
EXAMPLE::: Customize the output
---------------------------------
WS5100(config-wireless)#service wireless custom-cli sh-wi-radio ap-locn num-mu ap-mac channel power
WS5100(config-wireless)#sh wireless radio
AP LOCATION        #MU AP MAC              CHANNEL  POWER
San Jose 1st floor  0    00-15-70-15-11-62  40 (40 ) 4 (4 )

EXAMPLE::: Back to default
---------------------------
WS5100(config-wireless)#no service wireless custom-cli sh-wi-radio WS5100(config-wireless)#sh wireless radio
IDX   AP MAC             RADIO-BSSID       TYPE  STATE    CHANNEL  POWER  ADOPTED-BY
1     00-15-70-15-11-62  00-15-70-14-52-3C 11a   normal   40 (40 ) 4 (4 ) current-switch
```

NAS identifier

```
“nas-id” can now be globally set using the command: WS5100(config-wireless)#nas-id "my-string"
 The user can also override the nas-id on per WLAN basis using: WS5100(config-wireless)#wlan 1 nas-id "my-
string"
```

New CLI command to view the Signal, SNR and Average Data Rate as a summary table for all Mobile Units

```
WS5100#sh wireless mobile-unit statistics summary /---------------------+----+-----------------------------
----------+----------------------------------------\
|Mobile Unit Mac /    |    |           last 30 seconds               |           last 60 minutes
|
|       Name          |Wlan|Signal | Noise |  SNR  |Avg Rate |Retries|Signal | Noise |  SNR  |Avg Rate
|Retries|
+---------------------+----+-------+-------+-------+---------+-------+-------+-------+-------+---------+----
---+
|00-12-17-62-F8-31    |3   | -27.71| -92.14|  64.43|    6.00 |   0.00| -30.71| -92.71|  62.00|   38.15 |
0.01|
|00-18-DE-0C-6E-6D    |3   | -55.43| -94.29|  38.86|    6.00 |   0.00| -45.29| -94.14|  48.86|   14.43 |
0.00|
|00-15-AF-EF-1C-C7    |3   | -24.57| -91.43|  66.86|   54.00 |   0.00| -24.43| -92.43|  68.00|   53.51 |
0.15|
|00-07-40-FA-D3-85    |3   | -38.14| -84.43|  46.29|   54.00 |   0.00| -37.71| -90.86|  53.14|   46.63 |
0.06|
\---------------------+----+-------+-------+-------+---------+-------+-------+-------+-------+---------+----
---/
```

Note: Please note that WS51000 v3.3.1.0-003R software update can be applied only to the WS5100 switch.

2 RF Firmware Versions & Compatibility Matrix

Access Point/Access Port	Firmware Version
AP300	00.02-31
Layer 3 AP300	01.00-2144r
WIPS Sensor Image for AP300	00.00-04
AP100	02.05-00
AP4131	07.00-08
AP4131 Revert	00.00-00
Adaptive AP Image for AP-5131 (ADP image)	2.2.1.0-004R

For the prior Wi-NG releases on the WS5100, please see compatibility matrix with Adaptive APs below:

WS5100	AP5131 802.11 a/b/g
v3.1	v2.0
v3.2	v2.1
v3.3.1	ADP v2.2.1 (Separate image)

Note: Please upgrade Adaptive AP 51X1 from 2.1.to ADP image v2.2.1 to work with v3.3.1 on the WS5100. Please be aware that for existing installations that have v2.1 on the AP51X1 as Adaptive, the v2.1 AP will not get adopted by the v3.3.1 switch but will appear in the 'un-adopted list' until user sets up the switch to push the ADP 51X1 v2.2.1 image.

3 Installation Guidelines

For accessing the Graphical User Interface (GUI) of the WS5100 switches, the following browsers (and Java versions) are supported:

- Internet Explorer 7.0 and 6.0 on Windows 2000, XP (JRE 1.4.2)
- Mozilla 1.4.3 on RedHat Linux (tested with JRE 1.5)
- Firefox 0.8 or higher on Windows 2000, XP (JRE 1.4.2)
- Firefox 1.0 on RedHat Linux (tested with JRE 1.5)

3.1 Upgrade Information

This build may be installed over the following software versions:

- 1.4.1.0-014R
- 1.4.2.0-005R
- 1.4.3.0-012R
- 2.0.0.0-034R
- 2.1.0.0-029R
- 2.1.1.0-006R
- 2.1.2.0-010R
- 2.1.3.0-010R
- 2.1.4.0-001R
- 3.0.0.0-267R
- 3.0.1.0-045R
- 3.0.2.0-008R
- 3.0.3.0-003R
- 3.0.4.0-004R
- 3.1.0.0-045R
- 3.1.1.0-007R
- 3.2.0.0-040R

V3.x.x cannot be installed over v1.1.x or v1.2.x software releases. Please upgrade to v1.4.x or later releases prior to upgrading to v3.x.x.

3.1.1 Detailed Firmware Upgrade Procedure

This section outlines the upgrade procedure to v3.3.1 (from one of the software releases mentioned above).

Upgrade Process from v1.4.x/v2.x:

The first step in the upgrade process is to save and convert the existing v1.4.x or v2.x configurations. There is a Windows based configuration utility provided as part of this release to help in converting the older configurations to the newer (v3.x) format.

Install the configuration upgrade utility ("cfgupgrade-1.0.23-setup.exe") on a Windows System and follow these steps:

- Using TFTP or FTP copy the configuration file that you want to convert from the WS5100 wireless switch to the Windows System where the conversion utility is installed.
- On the Windows System click on "WS5100 Configuration Upgrade" icon, select the config file copied on to the Windows system and run it.
- A folder with the same name as the config file will be created.
- The folder will contain the converted startup-config file in v3.x format along with other log files.
- Using TFTP or FTP copy this startup-config file back to the WS5100 that you want to upgrade.

Please note that some of the Network access policies configuration items from older releases may not be converted into the newer format. In these cases it is recommended to build the new v3.x configuration from scratch.

Running the pre-upgrade script (preUpgradeScript) is recommended prior to upgrade to clean up the DOM to ensure sufficient memory for the upgrade. The pre-upgrade script and the upgrade have to be done independently.

1. Copy the appropriate pre-upgrade script file to the switch (using FTP or TFTP):

2. Enter “Service” mode CLI
3. “execute” the script file.

The steps to upgrade to v3.3.1 from either v1.4.x or v2.x are as follows. The method described in this section uses the Command Line Interface (CLI) and the Auto-Install procedures. To log into the CLI, either SSH, Telnet or serial access can be used (whichever exists).

4. First convert and save your existing configuration files using the Configuration Conversion Instructions (outlined above)
5. Copy the appropriate upgrade image file to the switch:
   - For upgrading from v2.x copy (via FTP or TFTP) the v2.x image upgrade file (WS5100-3.3.1.0-003R.v2).
   - For upgrading from v1.4.x copy (via FTP or TFTP) the v1.4.x image upgrade file (WS5100-3.3.1.0-003R.v1)
6. Enter “Service” mode CLI
7. “execute” the copied image file.
8. Restart the switch.
   - From CLI the command is “reload”.

Upgrading from a 3.0 engineering/beta build to 3.x released build:

1. Copy the executable patch file SigningCerts.patch to appropriate directory on the FTP/TFTP server to be used for WS5100 f/w upgrade/downgrade.
2. Install the patch file SigningCerts.patch from CLI or Applet by executing upgrade command from CLI or using Switch-> Firmware->Update Firmware option from switch applet
3. Please ensure the patch is properly installed from the output of the CLI command “show version”. The Patch file name should appear with the current f/w version string. The entry for the installed patch should also be displayed under the Patch section of the Switch-> Firmware screen in the applet.
4. Now the current f/w image is compatible for upgrading to 3.x Released Firmware.

Please follow the steps below.

Upgrading from a previous v3.x.x released version to 3.3.1.0-003R

1. Copy the WS5100_v3.3.1.0-003R.img to your 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”.

3.2 Auto-Install Process

Auto Install in v3.3.1 works via the DHCP server. This requires the definition of a Symbol/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 WS5100 ip address to where a L3 AP300 RF port or Adaptive AP 51X1 will be adopted
- Option 190 - defines the cluster config path and file name.

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 no, the URLs and the version default to "" (blank)

```
WS5100(config)#show autoinstall

feature    enabled      URL

config       no         --not-set--

cluster cfg  no         --not-set--

image        no         --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:

```
WS5100>en
```

```
WS5100#conf t
WS5100(config)#autoinstall image
WS5100(config)#autoinstall config
WS5100(config)#autoinstall cluster-config
```

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

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.

```
WS5100(config)#autoinstall config url ftp://ftp:ftp@192.9.200.1/ws5100/config

WS5100(config)#autoinstall cluster-config url
ftp://ftp:ftp@192.9.200.1/ws5100/cluster-config

WS5100(config)#autoinstall image url
ftp://ftp:ftp@147.11.1.11/ws5100/images/WS5100.img

WS5100(config)#autoinstall image version 3.3.1.0-003R

WS5100(config)#autoinstall config

WS5100(config)#autoinstall cluster-config

WS5100(config)#autoinstall image

WS5100(config)#show autoinstall

feature    enabled      URL

config       yes        ftp://ftp:ftp@192.9.200.1/ws5100/config

cluster cfg  yes        ftp://ftp:ftp@192.9.200.1/ws5100/cluster-config

image        yes        ftp://ftp:ftp@147.11.1.11/ws5100/images/WS5100.img

expected image version  3.3.1.0-003R
```

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--**.

3.3 Downgrade Procedure

It is possible to downgrade a switch running v3.3.1 image to one of the following versions **(Note: Only a non-RoHS version of the WS5100 hardware can be downgraded to v1.4.x and v2.0)**:

- 1.4.1.0-014R
- 1.4.2.0-005R
- 1.4.3.0-012R
- 2.0.0.0-034R
- 2.1.0.0-029R
- 2.1.1.0-006R
- 2.1.2.0-010R
- 2.1.3.0-010R
- 2.1.4.0-001R
- 3.0.0.0-267R
- 3.0.1.0-145R
- 3.0.2.0-008R
- 3.0.3.0-003R
- 3.0.4.0-004R
- 3.1.0.0-045R
- 3.1.1.0-007R
- 3.2.0.0-040R

Please follow these steps to **downgrade your WS5100 from v3.3.1.0-003R to v2.x or v1.4.x**

1. Make a note of the **license key; this will need to be re-installed**.
2. After downgrade, the switch will be in "out of box" configuration of the selected firmware version. Please save your existing configuration files to re-install after the downgrade.
3. Enable Portfast/Edgeport on the L2 switch where AP is connected
4. Reset the AP ("radio all-11a reset-ap")
5. Downgrade the switch using the following command (#upgrade tftp://ip-address/x.img) from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
   a. For downgrading to v2.1.4 use WS5100-2.1.4.0-001R.img file.
   b. For downgrading to v2.1.3 use WS5100-2.1.3.0-010R.img file.
   c. For downgrading to v1.4.3 use WS5100-1.4.3.0-012R.img file.
   d. For downgrading to v1.4.2 use WS5100-1.4.2.0-005R.img file.
6. Restart the switch. From CLI the command is "reload".

Please follow these steps to **downgrade your WS5100 from v3.3.1.0-003R to v3.x.x**

1. Use regular upgrade command to downgrade to 3.0.x.0 or 3.x.x.0-0XXR f/w version.

***NOTE:** **If you have a switch running v3.3.1.0-003R with no previous upgrade history, then please use the downgrade process described below to go to v3.x.x:**

Follow this step if downgrading to 3.x.x:

1. Copy the executable patch file *SigningCerts.patch* to appropriate directory on the FTP/TFTP server to be used for WS5100 f/w upgrade/downgrade.
2. Install the patch file *SigningCerts.patch* from CLI or Applet using steps similar to that for f/w upgrade [that is executing upgrade command from CLI or using Switch-> Firmware->Update Firmware option from switch applet]
3. Make sure that the patch is properly installed from the output of the CLI command "show version". The Patch file name should appear with the current f/w version string. The entry for the installed patch should also be displayed under the Patch section of the Switch-> Firmware screen in the applet.
4. Now the current f/w image is compatible for downgrading to 3.x.x.
5. Use regular upgrade command to downgrade to 3.x.x.0 f/w version.

4 Important Notes

1. 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.
2. For customers using WMM-TSPEC clients, please enable through CLI: *wireless admission-control voice enable.*
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. For existing customers that were using Self Healing, Motorola has now introduced the SMART RF functionality. Both features cannot be used simultaneously. Please note that SMART RF also provides Neighbor recovery and Interference Avoidance.
5. When entering MU MAC name, please do not exceed 63 characters on the WS5100.
6. For the Adaptive AP, ***the Independent and Extended WLANs must be on unique VLANs***.
7. With the Adaptive AP, the number of VLANs/WLANS supported is 15.
8. 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.
9. In case of login issues to the applet, it is recommended to clear the java cache for the browser
10. ***When manually adding radios for Adaptive APs on the wireless switch, please specify AP5131 where appropriate. The AP 300 is the default value.***

With v3.3.1, the model is similar to v3.0, where the WS5100 behaves more like a real wired bridge:

- Port assignments are not static or configurable. So both APs as well as wired devices can be connected on either port (or even both ports: you can divide your APs half-and-half, with some of them connected on eth1 others on eth2)
- The default port configuration is now **access** instead of **trunk**. The native VLANs are 2100 on eth1 and 1 on eth2

MAC Addresses

Like many other networking devices (Eg: Cisco Catalyst switches) Wi-NG 1.1 uses the same MAC address for all traffic coming out of the device, irrespective of what port is used. This is the MAC address of eth2 on the WS5100. Older WS5100 firmware (version 1.4.x/2.x etc) used to use the MAC address of the port where the frame was being sent out of. Since each port is mapped to a unique VLAN, any L2 domain is only going to see traffic from one of these ports, so this works out ok. If the user is mapping a L3 SVI on the eth1 port, and marking it for DHCP, the DHCP request will contain the source MAC address of eth2.

VLAN Configuration

The default VLAN configuration on the device now has both ports in access mode (meaning untagged, no external VLANs). Internally all traffic on eth1 is tagged with VLAN 2100 (i.e., the native VLAN on port eth1 is 2100) and all traffic on eth2 by 1 (i.e. the native VLAN on port eth2 is 1).

To use trunking two things need to be done:

1. The *mode* of the port needs to be made trunked
2. The VLANs that are allowed on that trunk, need to be added to the interface.

The following CLI commands would add VLANs 1 and 44 to interface eth2:

```
configure terminal

interface eth2

switchport mode trunk

switchport trunk allowed VLAN add 1,44
```

Note that 1 also remains the native VLAN on this port (can be changed using the *switchport trunk native* command). This means that:

1. All untagged frames coming in on this port will be assigned to VLAN 1 on ingress and then processed.
2. All frames with a VLAN tag of 1, would have their tag stripped on egress (i.e. they will go out untagged)
3. Frames tagged with VLAN 44 will ingress/egress with the tag intact
4. All frames with any other VLAN tag will be dropped (Note: including VLAN 1. i.e.: if we receive traffic with a tag that matches the native-VLAN, that will be dropped. By definition native-VLAN implies untagged traffic).

To make traffic on VLAN 1 to also be tagged, you can change the tagging mode of the native VLAN using:

```
configure terminal

interface eth2

switchport trunk native tagged
```

Note that the entire configuration described above only makes the switch aware of the existence of VLAN 44. I.e. if you map a WLAN to VLAN 44, all traffic from that WLAN will be switched out on port eth2 with the VLAN tag 44. i.e., the switch participates in this VLAN at the L2 layer. To make the switch participate at layer 3 (i.e. lets say you want to assign the switch an IP address on VLAN 44, or to do DHCP, or to route traffic through this VLAN) you need to also create this VLAN at layer 3. i.e., create an SVI as shown in the following example:

```
configure terminal

interface VLAN44

ip address 192.168.44.123/24
```

This now creates an interface on the switch, which is on VLAN 44, and assigns the switch an IP address of 192.168.44.123. Now the switch can be pinged at this IP address on VLAN 44.

Recommended Configuration

The recommended or best-practice configuration remains putting APs on port eth1 and using eth2 for your management and rest-of-the-network. This provides a clear physical distinction between the trusted and untrusted sides of the network. In some very simple configurations the customers may choose to use only one port, and in that case eth2 is recommended, since VLAN 1 defaults to eth2.

5 Issues Resolved in this Release

The following defects have been fixed in this release.

SPR	DESCRIPTION
16481	Security vulnerability – possible access to system thru CGI
16482	Security vulnerability – possible access to system thru CLI
16452	Hotspot and trusted WPA WLANs co-existence problems on ADP5131.
16478	Wireless Switch with large number of ADP5131 connected crashes unexpectedly with out of memory errors
16581	PSK-WPA2-TKIP is not working with Intel 4965ag and Broadcom a/b/g internal WLAN adapters with ADP5131
Bug ID 54835	Some ADP5131s do not re-adopt properly after switch fail-over.
Bug ID 54834	Prevent sending roam notification over the air.
15064	Similar credentials for log on can be used multiple times simultaneously.
15883	LED behavior change with AP300 found in v3.2. Prior to firmware 3.2 the AP300 LEDs would only react to data transmitted or received on its own BSSIDs. The LEDs would only flicker when data was moving through the AP radios to the switch. In firmware 3.2 we introduced a new locationing feature. The addition of the new locationing feature is what has caused the LED status change. With this new feature the 802.11g radio is reacting to all BSSIDs in the environment rather than just its own. In areas where there are many wireless networks detected the LEDs will flicker non stop even when there is no data going through the APs to the switch. This behavior has now been corrected.
15926	LED Sequence for Fan and Temperature do not match documentation.
15958	Incorrect display of DHCP IP Address for wireless sensor.
15934	Switch is not able to connect more than 32 AAPs with dual radio
15995	Radius Accounting logging is not available in v3.2
16013	GUI doesn't present proper bandwidth allocation per WLAN
16057	AP-5131 operating as AAP will not beacon or respond to probes for 32 character SSID.
15148	Some of the v3.x switches have the different engineid for the snmpmanager, snmptrap, and snmpoperator thus causing problems during configuration import.
15260	When a device (like CA50) involved in a VoIP phone call reaches an end of coverage area, devices close to AP not involved in the call are starved for data
15576	Changing from WMM mode to Normal on switch, AP reports data for traffic with TIM bits set. When clients do a PS-Poll AP reports no data but continues to advertise TIM with data.
15587	– 426 Error received when pulling config from Windows 2000 IIS FTP
15674	A user who has Monitor only privileges is able to access enable mode and view the running-config.
15683	GUI Login Error User Authentication Failed Too Many Log-ins From The Same User
15835	When you do a 'show wireless radio statistics 6' the switch is interpreting the 6 as 60min instead of the radio index.
15856	Redundancy issue with TCP port when primary and standby switches are separated by a firewall. Documentation has been updated to reflect correct port range for firewall.
15882	AAPs do not show up in Unadopted List
15891	When you set the country code in the CLI to either JJ or JW the beacon transmits that same country code. Instead it should transmit JP as the valid country code in the beacon.
15954	If both options (43 & 189) are set in the DHCP scope, L3 adoption of AP300 is not working.
15992	Ports Down after start-up when MSTP instance name not 'My Name'
16025	WS5100 DHCP server wrong SVI (VLAN interface) IP association

SPR	DESCRIPTION
16098	Internal DHCP server set to infinite lease time offers lease expiration date ending in year 1901.
16156	Invalid RADIUS shared secret being pushed to adaptive AP-5131's.
16159	Doubling of the roam notifications are being generated on every roam during association and re-association.
15884	WS5100 - 3.2 - The "show int" command displays the MAC addresses of Eth1 and Eth2 incorrectly

8 Known Issues

CRID	DESCRIPTION	Resolution/Workaround
SPR 15628/15925	Multiple errors generated on the applet when accessing access port radio screen with a variety of different model laptops.	
SPR 16137	CPU load error message encountered under release 3.2	
SPR 16143	Telnetting to active cluster switch during extreme load - cli sometimes does not respond .	Please reboot the Switch.
SPR 16292	A tagged (Vlan) port accepts only tagged packets, it does not accept untagged packets	
SPR 16310	Password-encryption secret stays encrypted even after deleting startup-config and restoring switch to factory default	
SPR 16323	FW 3.2 - NTP is enabled and functional but the switch GUI shows it is disabled.	
SPR 16330	3.2 Internal FTP server access denied - missing support for NLST command	
SPR 15573	Wireless Filter CLI accepts range of 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF – this functionality is available through the CLI. There is a GUI mismatch.	
44103	Adaptive AP: 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
52588	Cluster GUI: when enabled though GUI, the configuration is not in running config	The "Enable Cluster GUI" flag is valid only for the session as long as the applet is open. The moment one closes the applet, one is no longer in the Cluster GUI mode. The paradigm used here is similar to that present in cli. When one logs into a switch, one has to enter enable -> conf t -> to get into the default mode, then to enter cluster cli mode one has to explicitly enter cluster-cli mode. But after one logs out of the switch, and then reconnects they will have to again start from the default mode.
52517	Roamed TSPEC MUs are admitted even when the configured max-roamed-mus count is zero and res-roam-perc is zero	The behavior is as 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

CRID	DESCRIPTION	Resolution/Workaround
		which are sending voice traffic. In this scenario, the max percentage is configured as 75% and max MUs is 2 on the new radio and hence it would accept ADDTS from 2 roamed MUs
52892	Enabling a new Wlan causes disassociation of all Mus connected to different WLAN with Manual WLAN mapping	Any config push to the AAP causes it to bring down all radios and reinitialize
52592	Cluster GUI: Customer cannot edit radio configuration for AP's not adopted.	
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.
41870	Rogue AP: Duplicate entries are recorded in the Approved and unapproved AP list if two detectors detect the same AP.	
45167	Adaptive AP: 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.
43606	User Account with a (') character in password causes login failure	Please refrain from using (‘) special character in the switch login password
44971	Adaptive AP: Adaptive AP cannot be adopted using the secondary IP address of a Switch Virtual Interface (VLAN interface).	Please use the primary IP address
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
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 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.
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.

CRID	DESCRIPTION	Resolution/Workaround
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.
50494	AAP: Hotspot authentication for independent WLAN, using AP5131's on-board RADIUS fails	Please use an external RADIUS or the Onboard RADIUS on the Wireless Switch.
50187	Detector APs may reboot when browsing through the Rogue AP report.	No network disruption, as this only affects detector mode APs.
48343	AAP/applet: User cannot select AP image from the GUI on AAP firmware page, for USBs.	The following USBs have been tested to work and do not have the problem: • Memorex traveldrive 2.0GB (USB 2.0) • Kingston DataTraveler 1.0BG • Memorex traveldrive 8.0GB (USB 2.0)
49475	Secondary LDAP Server doesn't failover when primary LDAP server is unreachable in the Radius authentication	The workaround for this problem is that the administrator has to delete the primary LDAP server manually.
48882	AAP FW Upgrade failed when upgrade file is on cf and ftp root dir is also cf	The upgrade image has to be named as "aap_fw_image" and be present in the root of cf or usb and the same external drive has to be configured as the ftp root to get this working.
48915	IPSEC - ISAKMP Aggressive mode settings doesn't works	This can be configured as follows to work: On SW1(IP 10.10.10.45) ======-============ crypto isakmp key 0 test12345 address 10.10.10.250 crypto map map2030 10 ipsec-isakmp set peer 10.10.10.250 match address aclstos set mode aggressive set transform-set tfset On SW2 (IP10.10.10.250) ========== crypto isakmp key 0 test12345 address 10.10.10.45 crypto map map2030 10 ipsec-isakmp set peer 10.10.10.45 match address aclstos set transform-set tfset set mode aggressive

CRID	DESCRIPTION	Resolution/Workaround
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".
49342	AAP: Deleted AAP radio will not be adopted after enabling adopt unconfigured radio.	This can be recovered by doing the following: • Delete the AAP. • Reboot the AAP. • Reboot the switch.
49356	RTLS: 'reader 1 antenna 1 power' doesn't really apply to the third party reader	Please set power levels directly on the reader.

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 page and the 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.