Release Notes for WS5100 v3.3.5.0-002R & ADP5131 v2.2.5.0-001R

Contents

1 Introduction

Version 3.3.5.0-002R is a maintenance update to the major software release v3.3 on the WS5100 wireless switch platform based on the Wireless Next Generation (Wi-NG) architecture. V3.3.5 includes fixes for certain defects that have been reported by customers and/or found internally.

V3.3.5.0 is supported only on the WS5100 wireless switch.

When upgrading to this major release at a customer site, it is recommended that it be applied to one WS5100, ensure that the switch is run through basic functionality tests to ensure that the customer network is operational, and only then upgrade all the other WS5100 systems.

2 RF Firmware Versions Supported

Access Point/Access Port	Firmware Version
AP300	00.02-31
Layer 3 AP300	01.00-2330r
WIPS Sensor Image for AP300	4.5.1.7
AP100	02.05-00
AP4131	07.00-08
AP4131 Revert	00.00-00
Adaptive AP Image for AP-5131 (ADP image)	2.2.5.0-001R

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

WS5100	AP5131 802.11 a/b/g	AP7131 802.11 a/b/g/n
V3.1	v2.0	N/A
V3.2	v2.1	N/A
V3.3.1	ADP v2.2.1 (Separate image)	N/A
V3.3.2	ADP v2.2.2 (Separate image)	N/A
V3.3.3	ADP v2.2.3 (Separate image)	N/A

Note: Please upgrade Adaptive AP 51X1 to v2.2.5 to work with v3.3.5 on the WS5100. The ADP-51X1 adaptive image is packaged within the download bundle of the Wireless switch images on http://support.symbol.com.

3 Installation Guidelines

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

- Internet Explorer 6.0, 7.0 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 or higher 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
- 3.3.1.0-003R
- 3.3.2.0-010R
- 3.3.3.0-006R
- 3.3.4.0-009R

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.x applicable if the RF switch has a beta release of v3.3.x or released v3.x installed.

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).

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 v3.3.5 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 (WS5100-3.3.5.0-002R.v2).
   - For upgrading from v1.4.x copy (via FTP or TFTP) the v1.4.x image upgrade file (WS5100-3.3.5.0-002R.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 previously released v3.x Release or beta build (v3.x.0.0-xxxB)

1. **Before you begin:**
   To update an existing WS5100 to version 3.3.5.0-002R, the WS5100 must be using version 3.3.4.0-009R or earlier release. When upgrading from engineering build – you might need to install SigningCert.patch first. 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.

2. **Before you begin (strongly recommended):**
   As a precaution, it is recommended that the current running configuration is saved and copied to a FTP/TFTP server before performing the upgrade.

3. **Copy the new system image file to your FTP server.**

4. **Upgrade to new system image:**
   From CLI: WS5100#**upgrade ftp://username:password@<ip address of server>/<name of file>**
   Or
   From GUI: **Switch->Firmware->Update Firmware**.

5. **Verify the Upgrade**
   After the WS5100 reboots, from the CLI, check the Software Ver. for 3.3.5.0-002R.

Downgrade Process for the WS5100 from this service release

Use steps 4 and 5 from upgrade process to downgrade this service release to prior release.

Upgrading ADP5131 to v2.2.5

The Wireless Switch can upgrade the Adaptive AP's either manually or automatically. 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 WS5100.

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/tftpserver.

2. Please switch to wireless mode. Then, configure the path to the Adaptive AP image file using command:
   WS5100(config-wireless)# ap-image ap5131 <path where the image file is copied>

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 3.3.5
   WS5100(config-wireless)#no aap auto-upgrade enable

2. Manually upgrade from the switch all Mesh client bridges (ADP5131)
   WS5100(config-wireless)#aap fwupdate n (where n is the ap index for the mesh client bridge) enable

3. Manually upgrade the Adaptive AP from the wireless switch by using the following command:
   WS5100(config-wireless)#aap fwupdate n-x (where n & x are the limits of the ap indexes) enable

The version of the upgrade APs can be verified by:

WS5100(config-wireless)#Show wireless ap<index of adopted aap> enable

Note: AP5131s can only be upgrade from v2.1 (on the AP) onwards to the follow-on Adaptive images. AP-5131's can be upgraded either manually from switch or Auto upgrade with the exception of Mesh client bridges which should always be manually upgraded.

3.2 Auto-Install Process

Auto Install in v1.x 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 WS5100 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.

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)

```
RFS-7000(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:

```
RFS-7000>enable
RFS-7000#conf t
RFS-7000(config)#autoinstall image
RFS-7000(config)#autoinstall config
RFS-7000(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.

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

```
RFS-7000(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.x.x.0-xxxR

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/S51000/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  3.3.5.0-002R
```

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

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. 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 15.
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. ***When manually adding radios for Adaptive APs on the wireless switch, please specify AP5131 where appropriate. The AP300 is the default value.***
10. Following characters are illegible for use for login and password: *, space character
11. ***Radius Server doesn't allow configuring two or more clients with /24 mask of same network***.
12. ***Prior to v3.3.4, AP5131/AP5181 model number was hard coded to ADP5131, so when radios of AP5131/5181 were added, it used to show up as ADP5131. This is fixed in this release, we no longer hard code the model number to ADP5131 instead model number is read from manufacturing ROM. So if you already have ADP5131 as model number in config file, those entries need to be removed and radios need to be added as AP5131/5181 depending upon the AP type.***
13. ***Prior to 3.3.4, if a standalone AP5131 is connected to the WS5100, the AP adoption is denied if there is no ADP image on the Switch and auto-upgrade is disabled. The idea is to push the ADP image to the AP and AP comes up with ADP firmware and gets adopted. This restriction is removed in 3.3.4, standalone AP5131 gets adopted to the WS5100 and the user is responsible to upgrade to ADP image.***

5 Issues Resolved

The following SPRs were resolved as part of v3.3.5 release on WS5100:

SPR	Description
19725	With WS5100 v3.3.4/AP300, in few instances EAPOL packet is getting sent before Association Response.
19394	With Pre-authentication enabled on a WLAN, when the pre-authentication capable client doing EAP tries to connect to that WLAN, CCServer core is generated.
19787	Even though http server configuration is enabled in running-config, the check box for "Enable http" is shown as unchecked from GUI. CLI reports HTTP server as not running.
19927	Certificate signing requests generated with 2048 bit RSA keys are actually using 1024 bit keys.
20164	CCServer crashes when MU roams away during dot11i key rotation.
20460	From GUI, DHCP relay parameters are not configurable.
20439	The System partition is running out of free space because of dhcpd.leases file grows to 8MB filling up that partition. It causes onboard DHCP server failing to issue any further leases.
19693	With WS5100 v3.3.3/ADP5131 v2.2.3 - Calling station MAC address format does not conform to RFC-3580 IEEE 802.1X radius usage guide lines. As per these guide lines, calling station MAC address format needs to be separated by Hyphen instead of Colon.

6 Known Issues

CRID/SPR	DESCRIPTION	Resolution/Workaround
56823	In active-standby configuration – standby switch sometimes shows high CPU load erroneously	
52892	Enabling a new Wlan causes disassociation of all Mus connected to different WLAN with	Any config push to the AAP causes it to bring down all radios and reinitialize

CRID/SPR	DESCRIPTION	Resolution/Workaround
	Manual WLAN mapping	
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.	
52687	Wireless: cli command "dhcp-one-portal-forward" prevents CB3000 wired clients to receive DHCP address	Please disable dhcp-one-portal-forward command
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.
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

CRID/SPR	DESCRIPTION	Resolution/Workaround
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.
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
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.
49342	AAP: Deleted AAP radio will not be adopt 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.

d. Access Port(under Network sash, choose Access Port and the 'Adopted AP' tab)

Display: Same as Wireless LAN.

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 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.