WiNG 5.6.0.0-056R Release Notes

Overview

Motorola Solutions is pleased to announce the launch of the WiNG 5.6 software release. WiNG 5.6 adds significant new features and functionalities in the areas of Internetworking, Standards and Security. WiNG 5.6 also introduces support for the new AP 8163 access point and 802.11n 3rd radio sensor module on AP 8232 access points. WiNG 5.6 is enabled across the Portfolio of Access Points, Wireless Controllers and Integrated Services Platforms.

The VX 9000 Virtualized WLAN Controller platform is also being introduced with WiNG 5.6. See PMB 2416 - VX 9000 Launch Announcement for additional details including demo vs production images, and licensing and hypervisor support.

AP 8163 is being released as on outdoor hotspot, MCX and other outdoor features will be in the next WiNG release. See PMB 2401 – AP 8163 Launch Announcement for additional details.

Notes:

1. The NX 7500 platform is being released with WiNG 5.5.2 at roughly the same time as WiNG 5.6 and will not be supported with WiNG 5.6.
2. WiNG 5.6 is intended to be used with ADSP 9.1.1
3. AP 8232 will support the 3rd radio sensor module with ADSP 9.1.1
4. WiNG 5.6 is based on WiNG 5.5.1 and includes all critical bug fixes and SPRs fixed in 5.5.1. In addition, most SPRs and critical bugs fixed in WiNG 5.5.2 have been included in WiNG 5.6 as well.

1. Platforms Supported

WiNG 5.6 supports the following platforms with the corresponding firmware images. Note: Virtual Machine capability is supported on NX 45XX, NX 65XX and NX 95XX controllers only.

Controller Platform	Firmware Image
RFS 4010 / RFS 4011	RFS4000-5.6.0.0-056R.img, RFS4000-LEAN-5.6.0.0-056R.img
RFS 6000	RFS6000-5.6.0.0-056R.img, RFS6000-LEAN-5.6.0.0-056R.img
RFS 7000	RFS7000-5.6.0.0-056R.img, RFS7000-LEAN-5.6.0.0-056R.img
NX 9000	NX9000-5.6.0.0-056R.img (image without VM support)
NX 9500/ NX 9510	NX9000-5.6.0.0-056R.img (image without VM support)
NX 9500/ NX 9510	NX9500-5.6.0.0-056R.img (image with VM support)
NX 45XX/ NX 65XX	NX65XX-5.6.0.0-056R.img

AP Platforms	Firmware Image
Dependent APs	
AP 300	01.00-2354r (included in the RFS controller images)
AP 621	AP621-5.6.0.0-056R.img (included in all Controller images)
AP 622	AP622-5.6.0.0-056R (included in all Controller images)
AP 650	AP650-5.6.0.0-056R.img (included in all Controller images)
Independent /Adaptive APs	
AP 6511	AP6511-5.6.0.0-056R.img (included in NX controller images)
AP 6521	AP6521-5.6.0.0-056R.img (included in all Controller images)
AP 6522	AP6522-5.6.0.0-056R.img (included in all Controller images)
AP 6532	AP6532-5.6.0.0-056R.img (included in all Controller images)
AP 6562	AP6562-5.6.0.0-056R.img (included in all Controller images)
AP 7131 / AP7161 / AP 7181	AP71XX-5.6.0.0-056R.img (included in NX controller images)
AP 8132 / AP 8122/ AP 8163	AP81XX-5.6.0.0-056R.img (included in NX controller images)
AP 8222 / AP 8232	AP82XX-5.6.0.0-056R.img (included in NX controller images)
Independent /Adaptive Wall Switch	
ES 6510	AP6511-5.6.0.0-056R.img (ES 6510 uses AP 6511 image)

Virtualized WLAN Controller	Firmware Image
VX (WiNG as a VM) – production iso image	VX9000-INSTALL-5.6.0.0-056R.iso
VX (WiNG as a VM) – demo iso image	VX9000-DEMO-INSTALL-5.6.0.0-056R.iso[1]

Note 1: The VX demo image is a 60-day trial image of the VX-9000 software VM that can be used for demos and in the lab environments. This image does not need any additional licenses; it comes with 16 AAP licenses built-in. There is no migration from the demo image to the production image.

2. New Features in WiNG v5.6

WiNG 5.6 introduces support for the following new features.

Network Management	
Hierarchical Management for T5 WiFi over VDSL solution	Adopt, provision, push firmware and monitor a T5 WiFi over VDSL network alongside WiNG APs. Supports T5 Switch model TS-524 and its dependant TW-51x devices. This is useful in hospitality and related MDU vertical market. It requires an Adaptive AP license for every managed T5 Switch model TS-524.
AP Adoption Steering for multi-cluster deployments	In a large multi-cluster scenario, the default controller discovery FQDN (motorola-wlc.xxxx) resolves to a steering controller. The steering controller uses auto-provisioning policy match criteria options to direct the APs to the appropriate NX 95xx cluster for adoption and to upgrade AP firmware. This is required in very-large multi-cluster network deployments (larger than 10,240 APs). Supported with the NX 95xx controllers.
Increased cluster size of 6	Increases the maximum cluster size from 2 to 6 for purposes of license sharing, AP load balancing between WLAN controllers. Assists WiNG 4 customers using larger cluster sizes to migrate to WiNG 5. The configuration migration tool is also enhanced to assist with migration. Supported on the RFS 4000, RFS 6000 and the RFS 7000 controllers.
Device Provisioning Admin Role	New admin role that allows the user to add/ delete/modify device entries but not change profiles/ rf-domains objects. Assists in deployment, without operational impact to the rest of the network. Supported on all platforms.
Security	
Enhanced Base WIPS	WiNG 5 base WIPS functionality is being enhanced to support rogue AP classification using wired side detection, termination, and rogue detection of APs leaking wired traffic from a sanctioned network. The Advanced WIPS License on WLAN controllers is being terminated and replaced with this feature to simplify WLAN WIPS offerings. Supported on all WLAN controllers.
Certificate Management Protocol (CMP v2)	Support for CMPv2 protocol for device certificate management. CMP is the protocol for communication with a CA and assists in renewal of certificates automatically on expiry/ preconfigured time, on adoption or manually when initiated by the administrator.

Wireless	
Controller Assisted Roaming	Roaming enhancements to provide WLAN controller assistance when there is no direct connectivity between the access points as in conventional WiNG 5 deployments. Controller caches roaming information from one access point and provides it to another access point over GRE tunnels that are set up between the controller and the access points.
Captive Portal: Time Based Voucher	Allows a web admin to generate and print a voucher for a guest user that grants the user access for a specified period of time. Also contains the capability to generate vouchers in bulk for multiple users. This is particularly useful in retail and enterprise guest access scenarios, where admins want to pre-generate these vouchers to be handed out later. Limited to Active: Standby deployments. Supported on all WLAN controllers.
Usability	
PDF Reports	Several new PDF reports have been added to WiNG 5 corresponding to the Analytics functionality. The 50+ new reports span areas of measured traffic, captive portal, Smart RF, WIPS at a System, RF domain and AP level. This results in higher ROI as previously, ADSP was required to generate similar PDF reports.
Remote Packet Capture	Enhances the UI with remote packet capture capabilities, previously available only via the CLI. Provides the ability to take offline or live packet captures at the device and RF domain level. Simplifies remote debug with WiNG.
Mesh and Outdoor	
DFS Scan Ahead	DFS Scan Ahead helps minimize network disruption when an AP operating on a DFS channel experiences DFS radar detection. Channel change is anticipated to another DFS channel, which would otherwise require Channel-Availability-Check (CAC) delay (potentially in minutes) prior to switching to the new channel. This is supported on the tri-radio version of the AP 7161 currently supported with ETSI domain.
Dual 5GHz radio support for AP 7161	2 radio 5 GHz support on AP 7161. When deploying 2 radios on the 5 GHz band the user will need to separate antennas to mitigate interference.
Internetworking	
Bonjour Gateway	Adds a gateway that supports Apple Bonjour protocol across subnets, so that Apple devices can automatically discover printers and other services. Useful in campus wireless deployments to support BYOD. Supported on all controllers and access points with the exception of AP 300.
Wired Captive Portal	Enables captive portal functionality for traffic originating from wired clients directly or indirectly connected to a Motorola WLAN controller - the WLAN

	controller needs to be on the traffic path. In a mixed mode deployment where the WLAN network is comprised of access points from multiple vendors, it enables the captive portal functionality to be enforced at a single point in the network – at the Motorola WLAN controller. Supported on all controllers.
Wired Rate Limiting	Limts the rate of traffic over L2TPv3 tunnels using configured rate limits in each direction. This provides an effective mechanism to control the WAN bandwidth usage. Supported on all controllers and access points with the exception of AP 300.
Standards	
Internet Protocol Version 6	Adds dual stack (IPv4 and IPv6) capability to WiNG including IPv6 based Captive Portal, Firewall, SLAAC. Supported on all controllers and access points with the exception of AP 300.
eBGP Support	Support for the Exterior BGP routing protocol on the NX 45xx and NX 65xx platforms so it can function as an external routing gateway to route to other AS. Supported on the RFS 40XX, RFS 60XX, NX 45xx, NX 65xx and the NX 95XX controllers.

New Platform Support

VX - WiNG as a VM	Delivers virtualized Wi-NG that can be hosted at Data Centers or cloud hosting platforms (e.g. Amazon). VX provides an alternate solution to deploying a physical WLAN controller when customers have a server deployed at each remote site, resulting in reduced hardware costs. Dataplane support is available for small VM instances up to 100 APs. With larger instances, the VX is limited to providing control and management functionality only.
AP 8163	Outdoor tri-radio 11n Access Point.

Software support for new modules:

- Support for the 802.11n 3rd radio sensor module on AP 82xx.

Licensing Changes:

End of Life announcements for the following licenses are being made via separate PMBs.

1. Analytics License (part number: NX-9000-ANLYTC-LIC)
2. Advanced Wireless Intrusion Protection License (part numbers: RFS-XXXX-ADWIP-LIC or NX-XXXX-ADWIP-LIC).

3. Firmware upgrade – Controllers and Dependent APs

3.1 Important Notes on upgrade/ downgrade

1. Use of “Lean Controller images” which were introduced in WiNG 5.5 is recommended in ONEVIEW/ hierarchical management network deployments.
2. When upgrading WiNG v4.x networks to WiNG v5.6, the deivce will not retain the 4.x configuration. Please use the configuration migration utility to convert a 4.x configuration to a v5.6 based configuration. This is an offline tool that assists with config migration. It is included in the zip file.
3. When downgrading from WiNG 5.6 to a version prior to WING 5.4.x through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:

   `device-upgrade rf-domain <RF domain name> all no-reboot` … this downgrades all APs (including the RF domain manager) without rebooting them

   `reload on <RF domain name>` … this reboots the entire RF domain.

   Staggered reboot option is not supported in this downgrade scenario.
4. AP 622 v5.2.3.0-008R must be first upgraded to v5.2.3.0-040R before it can be upgraded to v.5.6
5. Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP or controller. Please allow time for devices to complete the upgrade. Where APs are powered through PoE connections to WLAN controllers, the controller needs to stay up during the upgrade process.
6. Both the controller and the AP should be upgraded to the same versions – a firmware mismatch can cause network disruptions and should be avoided. When upgrading, the controllers should be upgraded first and then the APs. When downgrading, the APs should be downgraded first, and then the controller.
7. Upgrade for AP 650 from WiNG 4.x to WiNG 5.4.x is NOT seamless and requires additional steps. AP should first be updated to any WiNG 5.2.x or 5.3.x image.
   Please set in the controller profile “service wireless ap6532 legacy-auto-update-image <PATH:/ap.img> to point to WiNG 5.2.x or WiNG 5.3.x AP 6532 image.

   For example:
   1. Copy AP650/AP6532 5.2 image on the RFS flash
   ```
   rfs4000-22A1B8#copy tftp://<Server IP>/AP6532-5.2.0.0-069R.img
   flash:/AP6532-5.2.0.0-069R.img
   ```
   2. User the below command to first upgrade the AP650s to a 5.2 image
   ```
   rfs4000-22A1B8#configure terminal
   ```
   Enter configuration commands, one per line. End with CNTL/Z.
   ```
   rfs4000-22A1B8(config)#self
   rfs4000-22A1B8(config-device-XXX)#service wireless ap650 legacy-auto-
   update-image flash:/AP6532-5.2.0.0-069R.img
   ```
   3. If auto upgrade is enabled AP650 will get upgraded to 5.4.x once it adopts to the controller, else use the below command to upgrade the AP6532s to 5.4.x
   ```
   rfs4000-22A1B8#ap-upgrade ap650 <DEVICE>
   ```

8. In Virtual Controller deployments, APs running version 5.4 will not adopt to a virtual controller running version 5.5. First upgrade APs to version 5.5 (manually) and then upgrade the Virtual Controller. New APs need to be upgraded to 5.5 manually before connecting to a WiNG 5.5 Virtual Controller network.

9. Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

3.2 Upgrade/ Downgrade Matrix

This section documents allowed upgrade/ downgrade combinations. Please ensure that the controller and AP are on the same WiNG version after the upgrade is complete.

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
RFS + AP 650/AP 300	V4.3.x onwards on the controller	V4.3.x onwards on the controller	AP 650 and AP 300 images are contained within the controller image
RFS + AP 7131/AP 7131N	V4.1.1 onwards on the AP V4.3.x onwards on the controller	V4.1.1 onwards on the AP V4.3.x onwards on the controller	AP 7131/AP 7131N v5.x image is not within the controller image
RFS + AP 6532	V5.1 onwards	V5.1 onwards	AP 6532 image is contained within the controller image
RFS + AP 6511	V5.1 onwards	V5.1 onwards	AP 6511 image is not contained within the controller image
RFS + ES 6510	V5.4 onwards	V5.4 onwards	ES 6510 uses the same image file as the AP 6511. The image is not contained within the controller image
RFS 4011 with AP 650	v5.1 onwards	v5.1 onwards	
RFS/NX 9XXX + AP 7181 Controllers need to be on 5.4 to be able to adopt AP 7181.	V5.4 onwards	V 5.4 onwards	Controller assistance is not available for upgrade from 3.2.2 to 5.4. This can be performed standalone or with Wireless Manager.
RFS/NX 9XXX + AP 7161	V5.1.1, v5.1.4, v5.2 onwards	V5.1.1, v5.1.4, v5.2 onwards	
RFS/NX 9XXX + AP 6521/AP 621	V5.2 onwards	V5.2 onwards	AP 6521 image is contained within the controller image
RFS/NX 9XXX + AP 6522	V5.4 onwards	V5.4 onwards	AP 6522 image is contained within the controller image
RFS/NX 9XXX + AP 6562	V5.4.4 onwards	V5.4.4 onwards	AP 6562 v5.x image is

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
			not within the controller image
RFS/NX 9XXX + AP 622	V5.2.3, V5.2.13 or 5.4 onwards.	V5.2.3, V5.2.13 or 5.4 onwards.	AP 622 image is contained within the controller image. WiNG 5.3.x does not support AP 622
NX 45XX/NX 65XX + AP 7131, AP 6532, AP 650, AP 6511, AP 6521, AP 621	V5.2.4, 5.4.2 onwards	V5.2.4	AP images are contained within the controller image
NX 45XX/NX 65XX + AP 7181, AP 7161, AP 6522, AP 622, AP 6562, AP 8132	V5.4.4 onwards	V5.4.4	AP images are contained within the controller image
RFS/ NX + AP 8132	V5.2.6, 5.4.2 onwards	V5.2.6, 5.4.2 onwards	AP 8132 image is not within the controller image
RFS/ NX + AP 82XX	V5.5 onwards	V5.5 onwards	AP 82XX images are not within the controller image
RFS/ NX + AP 8122	V5.5.1 onwards	V5.5.1 onwards	AP 8122 images are not within the controller image
RFS/ NX + AP 8163	V5.6 onwards	V5.6 onwards	AP 8163 images are not within the controller image
VX + all supported APs	V5.6 onwards	V5.6 onwards	

3.3 Important Notes for AP 300

Please note the following when upgrading an AP 300 from prior images to WiNG v5.2 with an RFS controller.

Upgrading From	Pivot Image	Comments
WS 2000 v2.2 or prior	Please upgrade to v2.3.3 and load the Wispe image of AP 300 before plugging in the AP 300 to a WiNG v5.4.0 RFS controller.	If migrating to an RFS controller, please upgrade RFS –AP 300 to WiNG v4.3 prior to upgrading to WiNG v5.4.0.
CC-5000	If migrating to an RFS controller, please upgrade RFS –AP 300 to WiNG v4.3 prior to upgrading to WiNG v5.4.0.	A direct plug in of an AP 300 from CC-5000 to an RFS running WiNG v5.4.0 will not work. Please upgrade to pivot image of WiNG v4.3 first.
WS5100	Please upgrade to WiNG v3.3.5 or later on the RFS to v4.3, and then plug in AP 300 in to WiNG	Please ensure that WiNG v4.3 is the interim upgrade step prior to going to WiNG v5.4.0

Upgrading From	Pivot Image	Comments
	v5.4.0 – a three step upgrade.	
RFS 4000/RFS 6000/RFS 7000	Please upgrade to WiNG v4.3 prior to upgrading to WiNG v5.4.0.	If the controller is on WiNG v4.3 or 5.1.x , then it can be directly upgraded to WiNG v5.4.0

3.4 Upgrade/Downgrade Procedure for WLAN Controllers

For customers upgrading from an earlier WiNG 5 release not requiring ONEVIEW, the procedure is the same as before.

For customers using ONEVIEW in WiNG 5.5, please see the WiNG 5.5 training for details of upgrade/ downgrade***. Note in particular the use of the "Lean Controller image" which does not include AP image***s – since the controller image size is now significantly larger than WiNG 5.4.x release.

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

3.4.1 Upgrade from WiNG v5.x to WiNG v5.6

1. Copy the RFSX000-5.5.X.0-0XXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<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 controller. From CLI the command is —reload.

3.4.2 Upgrade from WiNG v4.3.x (or higher) to WiNG v5.6

1. Copy the RFSX000-5.5.X.0-0XXR.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 controller. From CLI the command is —reload.

Note: *Please use ftp to upgrade to WiNG v5.6 on an RFS 6000, and not tftp, if using GE1.*

3.4.3 Downgrade to a WiNG v4.3.X (or higher) from WiNG v5.6

1. Copy the RFSX000-4.3.X.X-XXXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<ip address of server>/<name of file>** command from CLI or **Operations>Device Detail>Load Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the Controller. From CLI the command is —reload.

Please note: due to hardware refresh changes on controllers RFS7000, RFS6000 and RFS40XX, downgrade/upgrade to version that doesn't support new hardware components will be prevented. Following currently released version don't support new hardware: v5.0.x, v5.1.x. v5.2.0, v5.2.1, v5.2.2, v5.2.11, v5.2.3, v5.3.0, all versions prior to v4.4.1.

Configuration Restoration

On upgrade from 4.x to 5.x the 5.x controller will save the configuration from 4.x in another file on flash (so that 'startup-config' will point to the 5.x default startup-config). The configuration file from 4.x is renamed to startup-config-wing4. The password encryption file is also moved to /etc2/encrypt-passwd-wing4.

On downgrade from 5.x to 4.x the controller will save the 5.x configuration and it is moved to hidden files of the same name (/etc2/.encrypt-passwd-wing5 and /etc2/nvram/.startup-config-wing5). Any previously saved wing4 config if present (ie. startup-config-wing4) is restored back.

3.5 Upgrade/Downgrade Procedure for dependent APs connected to RFS controllers

3.5.1 AP 650 upgrade

If upgrading from any of the following releases 5.0.x, 5.1.x, 5.2.0.x, 5.2.1.x, 5.2.3.x, 5.2.4.x, 5.2.6.x, 5.2.11.x, 5.2.12.x, 5.2.21.x or 5.3.x, you need to upgrade to 5.2.13 or 5.4.x before upgrading to 5.5

A WiNG 5.x controller can upgrade an AP 650 running 4.x code to 5.x using the WISPe upgrade. This capability is enabled using "legacy-auto-update" command for the controller, either under the device or profile. The controller will first adopt the access point using the standard WISPE protocol messages (just as a 4.x controller would adopt it) and then download the new image to it, which would convert the AP to WiNG 5.x version of code.
Legacy-auto-update is enabled by default. If legacy-auto-update is disabled, use the following CLI instructions to enable the Legacy-auto-update feature:

```
rfs4000-22A136#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs4000-22A136(config)#profile rfs4000 default-rfs4000
rfs4000-22A136(config-profile-default-rfs4000)#legacy-auto-update
rfs4000-22A136(config-profile-default-rfs4000)#commit
rfs4000-22A136(config-profile-default-rfs4000)#
```

Important: In WiNG 5.4.x – please enable FTP server on the controller for legacy-auto-update to work.

The AP 650 can be automatically downgraded to a 4.x version of the AP by connecting it to a controller running the version 4.x. The AP tries to discover both 4.x as well as 5.x controllers by default, and if it does not find a 5.x controller, but does find a 4.x controller, then it will adopt to it, and as part of the adoption the 4.x controller will download a 4.x image to it.

Important: See also Section 4.1 Important Note #3

3.5.2 AP 7131 upgrade from AP 4.x

For AP 7131's running 4.x firmware the released 5.x firmware (AP71XX-5.4.x.0-.img) should not be used to upgrade the AP to 5.x. Instead for every 5.x release, there is a corresponding migration image to 5.x (AP7131-5.4.X.0-0XXR.bin).

3.5.3 AP upgrade options

WiNG 5.x supports AP firmware upgrade from the controller. For firmware upgrade from the controller, the AP firmware image should first be loaded on the controller; it can then be used to upgrade all access points of that type.

AP firmware images available on the controller can be checked using the following command:

```
rfs4000-22A1B8#show device-upgrade versions
```

If AP firmware is not part of controller image – new image can be uploaded using following command:

```
rfs4000-22A1B8# device-upgrade load-image ?
  ap621   Upgrade an AP621 device
  ap622   Upgrade an AP622 device
  ap650   Upgrade an AP650 device
  ap6511  Upgrade an AP6511 device
  ap6521  Upgrade an AP6521 device
  ap6522  Upgrade an AP6522 device
  ap6532  Upgrade an AP6532 device
  ap6562  Upgrade an AP6562 device
  ap71xx  Upgrade an AP71XX device
  ap81xx  Upgrade an AP81XX device
  ap82xx Upgrade an AP 82XX device
```

Once AP firmware is loaded on the controller, below are the different options that are available for AP firmware upgrade:

- **Manual Upgrade**

Firmware upgrade can be initiated on a single or a list of Aps using the below command.

```
rfs4000-22A1B8# device-upgrade ap71xx-16C7B4 ?
  no-reboot     No reboot (manually reboot after the upgrade)
  reboot-time   Schedule a reboot time
  upgrade-time  Schedule an upgrade time

rfs4000-22A1B8# device-upgrade ap71xx all ?
  no-reboot     No reboot (manually reboot after the upgrade)
  reboot-time   Schedule a reboot time
  upgrade-time  Schedule an upgrade time
```

- **Scheduling Firmware upgrade**

Firmware upgrade can be scheduled on a controller, that is upgrade time and reboot time can be configured. Firmware upgrade on the Aps follows the configured upgrade time.

```
rfs4000-22A1B8# device-upgrade all ?
  no-reboot     No reboot (manually reboot after the upgrade)
  reboot-time   Schedule a reboot time
  upgrade-time  Schedule an upgrade time
```

- **Upgrade through RF Domain manager**

Manual Firmware upgrade can be initiated through a domain manager

```
rfs4000-22A1B8# device-upgrade rf-domain default ?
  all     Upgrade all access points in rf domain
  ap621   Upgrade an AP621 device
  ap622   Upgrade an AP622 device
  ap650   Upgrade an AP650 device
  ap6511  Upgrade an AP6511 device
  ap6521  Upgrade an AP6521 device
  ap6522  Upgrade an AP6522 device
  ap6532  Upgrade an AP6532 device
  ap6562  Upgrade an AP6562 device
  ap71xx  Upgrade an AP71XX device
  ap81xx  Upgrade an AP81XX device
  ap82xx  Upgrade an AP82XX device
```

3.5.4 Auto Upgrade

Auto firmware upgrade can be enabled on the controller using the below command. Once this is enabled on the controller any AP that is being adopted to the controller if has a firmware version different than what is present on the controller gets upgraded to the version present on the controller.

```
rfs4000-22A1B8(config-device-XXX)# device-upgrade auto
```

The number of concurrent firmware upgrades can be configured using the below command based on the bandwidth available between the controller and the Aps.

```
rfs4000-22A1B8(config-device-XXX)# device-upgrade count ?
  <1-20>  Number of concurrent AP upgrades
```

Note: Auto upgrade on the APs always happens through the controller.

3.6 AutoInstall

AutoInstall in v5.4.X works via the DHCP server. This requires the definition of a Motorola Vendor Class and three sub-options that can be either sent seperately, or under option 43:
Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to entered as a string: —ftp://admin:motorola@192.168.1.10)

Option 187 - defines the firmware path and file name

Option 188 - defines the config path and file name

Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable “ip dhcp client request options all” on the vlan interface which is being used to perform the above autoinstall.
DHCP vendor class for platforms is noted below:

- MotorolaRFS.RFS4000
- MotorolaRFS.RFS7000
- MotorolaRFS.RFS6000
- MotorolaNX.NX9000
- MotorolaNX.NX4500
- MotorolaNX.NX4524
- MotorolaNX.NX6500
- MotorolaNX.NX6524

3.7 Virtual Machine Installation on NX 95xx/ NX 65xx/ NX 45xx

The ADSP VM can be installed on NX 95XX Integrated Series Controllers, it does not come pre-installed with WiNG 5.5.

There are no pre-installed VMs for NX45xx and NX65xx controllers.

The procedure to upgrade the VMs on these controllers is similar to the example below, except that it will always require first uninstalling the pre-installed VM.

Note: *The VM upgrade will not impact the currently installed/running VM. However, the "uninstall" will cause the VM's configuration and database entries to be wiped out. Please be sure to export and save the configuration and database prior to uninstalling.*

If the NX 95xx is running an image without VM support, first upgrade to the NX 95xx image with VM support. Follow the image upgrade process for WLAN controllers. This step is not required for the NX 45xx/ 65xx controllers. Then,

1. Download the ADSP image and place it onto an FTP/TFTP server or USB key
2. Using the ***upgrade*** CLI command or ***Firmware Upgrade*** option in the Web-UI, download the ADSP image onto the NX 95XX. Note if using the CLI it is recommended that you transfer the ADSP image to the NX 95XX using the background option! This will install the image in the /vmarchive partition.
3. Using the CLI ("virtual machine install") or App Center Install ADSP. The installation will take approximately 20 minutes to complete. Once installed the ADSP Virtual Machine will automatically start!

To upgrade a VM (instead of a first time install), you need to uninstall the currently installed VM and then install the new one. i.e. replace step (3) above with

```
NX9500#virtual-machine uninstall adsp      # Uninstalls the ADSP-VM
NX9500#virtual-machine install adsp        # Installs the new ADSP-VM
```

4. Firmware upgrade & Downgrade –Independent APs

4.1 Important Notes on upgrade

1. When downgrading from WiNG 5.6 to a lower WiNG 5.x version through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:

   `device-upgrade rf-domain <RF domain name> all no-reboot` … this downgrades all APs (including the RF domain manager) without rebooting them

   `reload on <RF domain name>` … this reboots the entire RF domain.

   Staggered reboot option is not supported in this downgrade scenario.
2. Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP. Please allow time for devices to complete the upgrade.
3. Upgrade for AP 6532 from WiNG 4.x to WiNG 5.6 is NOT seamless and requires additional steps. AP should first be updated to any WiNG 5.2.x or 5.3.x image.
   Please set in the controller profile “service wireless ap6532 legacy-auto-update-image <PATH:/ap.img> to point to WiNG 5.2.x or WiNG 5.3.x AP 6532 image.

   For example:

   - Copy AP6532 5.2 image on the flash

   ```
   ap6532-22A1B8#copy tftp://<Server IP>/AP6532-5.2.0.0-069R.img
   flash:/AP6532-5.2.0.0-069R.img
   ```

   - User the below command to first upgrade the AP6532s to a 5.2 image

   ```
   ap6532-22A1B8#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   ap6532-22A1B8(config)#self
   ap6532-22A1B8(config-device-XXX)#service wireless ap6532 legacy-auto-
   update-image flash:/AP6532-5.2.0.0-069R.img
   ```

   - If auto upgrade is enabled AP6532 will get upgraded to 5.4.x once it adopts to the controller, else use the below command to upgrade the AP6532s to 5.4.x

   ```
   ap6532-22A1B8#ap-upgrade ap6532 <DEVICE>
   ```
4. Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

4.2 Upgrade/ Downgrade Matrix

This section documents allowed upgrade/ downgrade combinations.

Independent/Adaptive Access Point	Upgrade from	Downgrade to	Notes
AP 6511	v5.1 onwards	v5.1 onwards	
ES 6510	v5.4 onwards	v5.4 onwards	
AP 6521	v5.2.x onwards	v5.2.x onwards	
AP 6522	v5.4 onwards	v5.4 onwards	
AP 6532	v5.1 onwards	v5.1 onwards	See Note 1
AP 6562	v5.4.4 onwards	V5.4.4 onwards	
AP 7131	v4.1.1 onwards	v4.1.1 onwards	
AP 7161	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	
AP 7181	v5.4 onwards	v5.4 onwards	See Note 2.

AP 8132	V5.2.6, 5.4.2 onwards	V5.2.6	
AP 8122	V5.5.1 onwards	V5.5.1 onwards	
AP 82XX	V5.5 onwards	V5.5 onwards	
AP 8163	V5.6 onwards	V5.6 onwards	

Note:

1. Note: If upgrading from any of the following releases 5.0.x, 5.1.x, 5.2.0.x, 5.2.1.x, 5.2.3.x, 5.2.4.x, 5.2.6.x, 5.2.11.x, 5.2.12.x, 5.2.21.x or 5.3.x, you need to upgrade to 5.2.13 or 5.4.x before upgrading to 5.5
2. AP 7181 - WLAN Controller assistance is not available for upgrade from 3.2.3 to 5.4.x. This upgrade can be performed standalone or with Wireless Manager. The migration process will convert the necessary settings/configuration to maintain mesh connectivity. Please refer to section 5.3.

4.3 AP Upgrade/Downgrade Procedure

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

4.3.1 Upgrade from WiNG v5.1.x or higher to WiNG v5.6

1. Copy the APXXXX-5.5.X-0XXR.img to your tftp/ftp server.
2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **AccessPoint->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the Access Point. From CLI the command is —reload.

Note: WiNG 5.1.3 added support for the new NAND for AP 7131N. WiNG 5.1.4 added support for the new NAND for AP 7161. Hardware revs with the new NAND will be unable to downgrade below these versions or version 4.1.5 – as these support the new NAND, but previous versions do not.

4.3.2 Upgrade/Downgrade for AP 7131/AP 7131N from WiNG v4.x to WiNG v5.x

Upgrade from WiNG v4.x to WiNG v5.x

If an AP 7131 has a firmware release version 3.2.0 or earlier, it is mandatory to upgrade the access point to release version 3.2.1.0 before an upgrade to release version 4.x or later can be attempted. Users on AP 7131 release version 3.2.2 need not downgrade to version 3.2.1 and can directly upgrade to a release version 4.x or later.

Users are strongly cautioned against upgrading from the AP 7131 System Boot OS prompt. Upgrading from the Boot OS prompt is not a recommended and supported upgrade methodology on the AP 7131.

To conduct a firmware update on the AP 7131 from the run-time system software
GUI:

1. Select ‘System Configuration’, ‘Firmware Update’ from the AP 7131 menu tree of the GUI.

2. Specify the name of the target firmware file within the 'Filename' field.
3. If the target firmware file resides within a directory, specify a complete path for the file within the 'Filepath (optional)' field.
4. Enter an IP address for the FTP or TFTP server used for the update.
5. Select either the FTP or TFTP button to define whether the firmware file resides on a FTP or TFTP server.
6. Set the following FTP parameters if applicable:
    a. *Username* - Specify a username for the FTP server login.
    b. *Password* - Specify a password for FTP server login.
7. Click 'Apply'.

Click the 'Perform Update' button to initiate the update. Upon confirming the firmware update, the AP reboots and completes the update. This step may take several minutes. After this upgrade the access point will reload and come up with wing 5.x firmware.

Note: *Please use the special "migration image" (**AP7131-5.5.X-0XXR.bin**) when upgrading from 4.x to 5.x.*

If the user upgrades an AP 7131/AP 7131N running a version of code older than 4.1.1.0 using the AP migration image, there is a possibility of the AP getting "stuck" on coming up with 5.x. If this occurs, the following error message is seen on the console after bootup:
cpu not running at correct speed. Expected(500Mhz) current> Speed(600MHz)
To work-around this issue, the administrators need to type the following command after the error message: 'achip fix-cpu-speed'
When the AP comes upto runtime, upgrade again using the 'upgrade' command to the latest 5.3 release.

Downgrading from WiNG v5.x to AP v4.x for AP 7131/AP 7131N

To downgrade an access point running 5.x back to 4.x the reverse migration image (AP7131-5.4.X-0XXR-040105000004R.img) needs to be used. This image is installed on the AP just as a regular 5.x firmware is installed using ap-upgrade/ device-upgrade from CLI or UI. Please refer to the AP 7131 v4.1.5 release notes for downgrade to an earlier version.

Downgrade the access points using the AP-upgrade/device-upgrade command from CLI of the AP and put all APs back to 4.x. All configurations from 5.x is lost as the AP is reverted to 4.x. However the original 4.x configuration, if any, could still be present on the AP.

Configuration Restore

Some of the configuration items from a 4.X AP 7131 are translated and migrated over to the 5.x version of the configuration after update. The items of configuration that are migrated are:

- Hostname
- Port phy configuration (speed, duplex)
- Port L2 configuration (trunking info)
- IP address of controller if available (translated to 'controller host' in 5.x)
- WAN interface IP addressing
- LAN interface /subnet1 IP address

If the configuration could not be read properly then the AP will come up with default 5.x configuration and create a logfile called legacyapn_<version>.dump.tar.gz in flash:/crashinfo indicating what was translated, what was the error etc, for post-analysis.

4.3.3 Upgrade/Downgrade for AP 7181 from v3.2.3 to WiNG v5.6.x

To upgrade an AP 7181 from v 3.2.3 to v 5.6, it must first be upgraded to v 5.4.x.
Likewise for downgrading AP 7181's from v5.6, it must be downgraded to 5.4.x before downgrading to 3.2.3.
Please see the WiNG 5.4 release notes and "WiNG 5.4 How-To Guide AP7181 Migration" on support central for the procedure.

4.4 AutoInstall

AutoInstall in v5.6 works via DHCP. This requires the definition of a Motorola Vendor Class and three sub-options that can be either sent separately, or under option 43:

Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to be entered as a string: —ftp://admin:motorola@192.168.1.10)
Option 187 - defines the firmware path and file name
Option 188 - defines the config path and file name
Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable "ip dhcp client request options all" on the vlan interface which is being used to perform the above autoinstall.
DHCP vendor class for platforms is noted below:

- MotorolaAP.AP6521
- MotorolaAP.AP6522
- MotorolaAP.AP6532
- MotorolaAP.AP6562
- MotorolaAP.AP6511
- MotorolaAP.AP7131
- MotorolaAP.AP7161
- MotorolaAP.AP7181
- MotorolaAP.AP8122
- MotorolaAP.AP8132
- MotorolaAP.AP8163
- MotorolaAP.AP8222
- MotorolaAP.AP8232

5. Important Notes

New in v5.6

1. NX 9500/ NX 9510 – When using the NX9500-5.6.0.0-056R.img (image with VM support) all resources are now allocated by default to WiNG. WING is allocated 32GB RAM at startup. To run the ADSP VM memory must first be freed up prior to installing the VM using the "`virtual-machine set wing-memory`", "`virtual-machine set vcpus`", and "`virtual-machine set disk-size`" commands followed by a system "`reload`". WiNG needs a minimum of 12 vCPUs, 16GB RAM and 500 GB of hard drive space is recommended for analytics.

2. AP 6511 – Firewall is disabled by default starting with WiNG 5.6 in order to meet the requirements for WiFi certification. Some features such as Captive Portal require firewall to be enabled.

3. IPV6 ACLs do not support the object oriented firewall feature in this release.

4. IPv6 implementation does not support IPsec VPNs in this release.

5. IPv6 – MLD snooping is not supported on the ethernet switch ports on the NX 4524 and NX 6524 platforms. It is supported only on UP1, UP2 ports.

6. IPv6 – When there are multiple DHCP servers (one for IPv4 and another for IPv6) that respond to option 191, ensure that both provide valid IP addresses/ hostnames. Otherwise, with both servers responding the later response will override the previous response. If the later response does not contain valid information, AP will not be able to adopt to the controller.

7. VX 9000 - Only 1 GE1 interface is supported on the VX platform

8. VX 9000 instances running in Amazon EC2 must use "Elastic IP" to retain the public IP when the instance is stopped and restarted.

9. VX 9000 - VMWare and other hypervisors need to be configured in promiscuous mode for features like VRRP to work correctly.

10. When creating a cluster between multiple VX 9000's, all instances should use identical resources (e.g. replication from one instance with higher memory to a smaller one can lead the smaller instance to run out of memory).

11. VX 9000 – Ipv6 is not supported when using Microsoft HyperV as the virtualization platform. Dataplane support does not work correctly with Microsoft HyperV. It works fine with other supported hypervisors.

12. Captive Portal Time Based Voucher is only supported with Active: Standby configurations. Active: Active based clusters are not supported. The database gets replicated from the Active Controller to the Standby Controller periodically (default is 5 min).

13. eBGP Scaling by platform is as follows:
    a. RFS4000/RFS6000 – 6000 routes

b. NX 9510 – 9000 routes
c. NX4500/NX6500 – 12 routes

14. T5 adoption – https must be enabled on the WiNG controller for T5 adoption to work

15. Wired Captive Portal
    - If wired captive portal is being used along with wireless captive portal on the same controller, then same captive portal policy needs to be used for both wired and wireless captive portal enforcement.
    - If Wired captive portal is being implemented for a particular bridged vlan on the controller's physical interface that receives APs traffic, then applying wireless captive portal for the same bridge vlan is not valid, since the wireless client will then be subjected to captive portal enforcement twice.

16. AP adoption steering notes:
    - AP images for upgrade should be hosted on the steering controller
    - Auto provisioning policy must be configured on the steering controller
    - Active: Active & Active: Standby modes are both supported in each target controller pair.

17. The following default values have been changed/ corrected:
    - *route-limit num-routes 12288 retry-count 5 retry-timeout 60 reset-time 1| route -limit num-routes 12288 retry-count 5 retry-timeout 60 reset-time 3* ….. reset time was changed from 1 to 3.
    - vrrp-state-check command previously present in "router ospf" context, has been moved to device/profile context
    - min-misconfiguration-recovery-time 120 …. Was increased from 60 to 120.

Introduced in version v5.5.x

18. Removing support for TKIP Encryption:

    Starting January 1, 2014, WPA TKIP is no longer permitted for Wi-Fi Alliance certified products. For AP/STA products wishing to support a legacy device that is capable of supporting only TKIP encryption, they are required to implement mixed mode with WPA/WPA2.
    Following changes are being implemented to comply with the above Wi-Fi Alliance requirement.

    a) Configuring encryption type as TKIP for a wlan will no longer be supported; WLANs that need to support TKIP clients should use TKIP-CCMP as the encryption type.
    b) Upgrading from a prior WiNG 5.x to release to WiNG 5.6 will automatically change the configurations for wlans using TKIP encryption to TKIP-CCMP and will add "service wpa-wpa2 exclude-ccmp" command to avoid any post upgrade incompatibility issues.

    For new configurations, to handle certain legacy/non-Wi-Fi compliant client situations where the client driver is incompatible or does not operate properly in a mixed mode TKIP-CCMP configuration, add the following command "service wpa-wpa2 exclude-ccmp" to the wlan configuration. This configuration allows the wlan to operate in TKIP only mode until the non-compliant wireless clients are phased out of the network.

19. WiNG 5.5.2 adds support for hardware refresh NAND component on AP 81XX and AP 82XX. Following restrictions will apply when using those APs with new hardware component:
    - New revision of hardware - downgrade/upgrade will only be supported to releases that also support those components. Downgrade/upgrade to all other releases will be prevented.
    - Older revision of hardware - downgrade/upgrade procedure is unchanged.

20. Change in behavior for "show wireless xxxxx" cli commands and techsupport for centralized controller deployments:
    For centralized controller deployments (multiple RF-Domains across distributed locations), all "show wireless xxxxx" commands will resolve only to the local rf-domain. This will prevent a "show wireless xxxxx" cli command without any rf-domain specified or a techsupport dump operation initiated on the centralized controller from collecting statistics information from all the distributed locations (rf-domains). New mechanisms have been added to collect rf-domain specific statistics individually or globally.

21. New Display Mode in the CLI to view RF-Domain specific or global (across all rf-domains) wireless statistics:

    From the CLI (in EXEC mode/privileged EXEC mode):

    "`on rf-domain <rf-domain_name>`" sets the display mode for wireless statistics show commands to resolve to a particular rf-domain, all "`show wireless xxxxx`" commands executed in this mode will automatically return the output corresponding to that rf-domain without the user specifying the "`on <rf-domain_name>`" extension to every command.

    "on rf-domain all" sets the display mode for wireless statistics show commands to run in global mode – i.e. for each "show wireless xxxxx" command that you run, the controller will display statistics across all rf-domains.

22. Ability to generate wireless stats summary report on a per rf-domain basis or globally (across all rf-domains):

    From the CLI (in privileged EXEC mode) –

    ```
    "service copy stats-report rf-domain <rf-domain-name> <URL>"
    "service copy stats-report global <URL>"
    ```

    Note: The above option can be utilized for generating inventory/reporting at a system level

23. Change in terminology for adoption/upgrade related action commands/events/traps:

    With WiNG 5.5 One View deployment scenarios supporting controllers to be adopted and managed by a centralized controller cluster, existing "ap-xxxxx" action commands have been replaced with "device-xxxxx" action commands. For example: ap-upgrade xxxx will now be referred to as device-upgrade xxxxx.

    All adoption related events and traps are modified to reflect the "device" terminology instead of "ap".

24. Ability to optionally include ‘dhcp client-identifier’ as part of DHCP Discover/Request packets:

    If your DHCP server uses dhcp client identifier for static bindings (dhcp lease reservations) and responds only to DHCP Discover/Requests with dhcp client identifier present, then the client identifier can be included by configuring the following command “dhcp client include client-identifier” under the SVI (interface vlan X) which is configured as DHCP client.

25. Auto-provisioning policy: ‘reevaluate-everytime’ command is modified to ‘evaluate-always’ and moved to ‘auto-provisioning-policy’ from device/profile context. Upgrade from 5.5.1 to 5.6 or later versions should work in accordance with location and syntax changes. However, downgrade from 5.6 to former versions would cause the command to disappear from all contexts.

26. NIST SP 800-131A regulation made 1028 bit certificates obsolete as of January 1, 2014. All self-signed on-board certificates which are 1028 bits will be regenerated upon upgrade. Customers need to upgrade all third party certificates to be compliant to new regulations.

27. “show global domain managers” will show incorrect values for number of APs if domain has APs on version below WiNG 5.5.

28. New images are introduced in WiNG 5.5 for the RFSxxx platforms. These images are labeled RFSxxx-LEAN-5.5.0.0-yyy.img. Where xxx is the target platform and yyy is the build version number. The new controller images do not include any AP images and are intended to be utilized on a site controller operating in a hierarchical typology.

    For a controller operating in a non-hierarchical setup, the upgrade process doesn’t involve copying the controller firmware to flash but rather it's copied to RAM. In this scenario, the traditional image (containing the AP images) can be used. However, in a hierarchical typology, during device-upgrade operation the controller image must be copied to flash. In this scenario the “lean" image must be used since the normal image does not fit in flash.

29. ONEVIEW – Site Controller and access points must be in the same RF domain.

30. New notation has been introduced for channel width for all APs in WING 5.5. The new model is to specify the primary channel followed by ‘w’ or ‘ww’ to indicate 40MHz or 80MHz. Please see the product documentation for details.

31. ADSP-WiNG Integration:
    - The ADSP release 9.1.1 Unified mode image that goes with WiNG 5.6 will be released separately later. Please see the ADSP release notes for resource requirements for ADSP when operating in Unified mode.
    - When ADSP is in Unified Mode, it periodically synchronizes with WiNG tree hierarchy. If there are no Areas or Floors under an RF-domain it will create an Area and Floor under that RF-domain automatically in the ADSP scope tree. If later, an Area and Floor are created under that RF-domain within WiNG, they are automatically synchronized into ADSP (including synchronization of device placements).
    - WiNG auto-provisioning rules have been expanded to include auto-placement of generic non-WiNG 5 devices. These rules are consumed by ADSP running in Unified mode to auto-place non-WiNG 5 and third party devices.

32. Leverage Level 2 MINT links when building out large multi-site deployments. This is not new in 5.5, but is a common issue when scaling large deployments. WiNG 5 uses Level 1 MINT links by default. There is direct communication between all Level 1 MINT neighbors increasing network traffic and database sizes on the WiNG nodes. Using level 2 MINT links summarizes this information, thereby creating a more efficient network design. Please see the NOC deployment guide for details.

33. WLAN controller does not retain saved auto upgrade configuration when downgrading from 5.5 to pre-5.5 release. This is because “ap-upgrade” commands were renamed to “device-upgrade” in 5.5. When upgrading to 5.5, the conversion happens automatically, however, when downgrading from 5.5 the previous firmware release does not understand “device-upgrade”. The workaround is to manually fix the configuration.

34. Mesh Connex Migration – With the introduction of Auto Channel Select, Mesh Connex Configuration will be migrated when the WLAN controller reboots. The following parameters get migrated:
    - Channel list from smart-rf is copied on to the rf-domain.
    - Priority meshpoint name and root recovery parameters are copied to the meshpoint-device configuration under device context or profile of the APs.
    - For Per-Area Smart RF, the channel list configured for that “Area” is directly configured to the device context of the APs which are part of that area.

35. Open up management access only to those subnets that the administrator will access the devices from. Leaving the management access open in general poses a risk to the network. This will also help eliminate known (medium/ low) vulnerabilities and unknown vulnerabilities that may be discovered in the future. At the time of the release there are no known high vulnerabilities (tested with Nessus/ Qualys Guard/ Tripwire-Purecloud)

36. Voice enterprise, Hotspot2.0, 802.11w and WIPS sensor features are currently not supported on AP 82xx Access Points. Add-on modules (e.g sensor, LTE) are not supported either. These features will be made available in a future release.

37. Following is a list of clients that were validated for use with AP 82xx access points

MODEL	CONNECTIVITY	BAND	PHY
Macbook Air(2013)	PCIe	ac+abgn	3x3:3
ASUS PCE-AC66	PCIe	ac+abgn	3x3:3
Broadcom 11n - Asus G750J	PCIe	ac+abgn	2x2:2
Edimax EW-7822UAC	USB 3.0	ac+abgn	2x2:2
Belkin F9L1106 v1	USB 2.0	ac+abgn	2x2:2
Netgear A6200	USB 2.0	ac+abgn	2x2:2
D-Link DWA-182 rev A1	USB 2.0	ac+abgn	2x2:2
Buffalo WI-U2-866D	USB 2.0	ac+abgn	2x2:2
Linksys AE6000	USB 2.0	ac+abgn	1x1:1
Asus AC1200	USB 2.0	ac+abgn	2x2:2
Zyxel NWD 6505	USB 2.0	ac+abgn	1x1:1

TRENDnet TEW-805UB	USB 3.0	ac+abgn	2x2:2

38. WiNG 5.5 extended L2tpv3 support for AP 6521, AP 621 and AP 6511. In addition on configuring l2tpv3 settings on those APs – following is required to be set in AP profile for l2tpV3 to work – “service l2tpv3 enable”.

39. WiNG 5.5 introduced addition of precedence to ip nat rules.

    ```
    ip nat inside source list mylist ?
      precedence  Set precedence of access list
    ```

    ```
    ip nat inside source list mylist precedence 1 interface vlan2 overload
    ```

40. In WiNG 5.5 legacy mesh related show commands have been replaced with ‘mint’ to remove confusion with meshpoint functionality. Use “show wireless mint links” to see the legacy mesh links.

41. Captive Portal Deployments using External (or) Advanced pages:

    Captive portal query string delimiter has been changed to ‘&’ instead of ‘?’ from WiNG 5.5 onwards. When upgrading to a 5.5.x based firmware, the JavaScript embedded in the external or advanced webpage(s) needs to be updated to parse the new style of query stings.

    Following line needs to be modified under function **getQueryVariable(variable),**

    var vars = query.split("?"); === change it to ==➔ var vars = query.split(/[?&]/);

    Please ensure that this function gets updated in all the captive portal pages that uses it.

<u>Introduced in version 5.4.x</u>

42. AP300 default setting changed to ACS instead of SMART which is not supported on AP300 platform.

43. Following vulnerabilities were addressed:

    CVE-2010-4478 - OpenSSH J-PAKE Session Key Retrieval Vulnerability

    CVE-2012-0814 - OpenSSH Commands Information Disclosure Vulnerability

    Note: even though vulnerabilities were addressed – some vulnerability scan firmware that only checks the version number of the component as opposed to testing the actual vulnerability – might still report issue being present.

44. Transmit power adjustments for following platforms:
    a. AP 6532 – Adjustments to FCC, ETSI, and Japan
    b. AP 8132 – Adjustments to FCC, ETSI, and Japan
    c. AP 622/AP 6522 – Adjustments to FCC & ETSI
    d. AP 6562 – Adjustments to FCC & ETSI

45. When upgrading from prior versions – new profiles for newly supported platforms will not be present in the startup-config. User can either create a default profile or do “erase startup-config”.

46. Mismatch in controller and AP version (v5.4.2 and below) will cause extended VLANs not to work properly.

47. ADSP SA cannot be run through a mesh with AP7131N tri radio; non root AP has 3rd radio as sensor

48. Interoperability with Samsung S2 devices:
    A Samsung Galaxy S2 device sometimes fails to connect using EAP-MAC authentication and WEP64 encryption. It's recommended to reduce the number of attempts (authentication eap wireless-client attempts) from default 3 to 2.

49. With 802.11r enabled WLAN – some clients might have problems associating. Please create a different WLAN for non 802.11r enabled clients.

50. ADSP Spectrum Analysis doesn't work over a mesh connection.

51. MCX max range feature – the maximum range is 25 km except for 5Ghz 40Mhz channels where range is 24km.

52. WiNG 5.4 and above enforces the limit of policies on standalone APs. Current limit for DHCP, L2TPv3 policy and etc. is one policy per AP. When upgrading from WiNG 5.3 where the limit was not enforced – only one policy will be maintained.

53. VMM – please use following recommendations when configuring VMM feature:
    - Disable L2 Stateful Packet Inspection in Firewall Policy
    - Disable Dynamic Chain Selection on the radio
    - Use Opportunistic Rate Selection on the radio
    - Disable A-MPDU Aggregation if vehicular speed is greater than 30 mph
    - Set RTS-Threshold to 1 on all mesh devices

    Note: for more detail use case scenarios see AP 7161 VMM How-To guide.

54. It's recommended disabling IP DoS attacks in firewall policy when configuring IGMP snooping.

55. 10 GbE support on the NX 9510 is limited to SFP+ SR interfaces that are included in the controller. LR or XR SFP+ are not supported.

56. NX 9510 only supports extended VLANs in version 5.4.2. L2TPv3 tunneling, IPsec VPN, are not supported in v 5.4.2. These features will be supported in a future release.

57. When downgrading from WiNG 5.4 to a lower WiNG 5.x version through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:
    ap-upgrade rf-domain <RF domain name> all no-reboot … this downgrades all APs (including the RF domain manager) without rebooting them
    reload on <RF domain name> … this reboots the entire RF domain.
    Staggered reboot option is not supported in this downgrade scenario.

58. The Firewall has been enhanced in 5.4 to a per-VLAN firewall which can be enabled or disabled on a per-VLAN basis. Per VLAN Firewall is enabled by default. It can be enabled using "firewall" cli command and disabled using the "no firewall" command.

59. WiNG 5.4 adds support for the new USB chip for RFS6000. Previously support was added for the new power supervisor chip.

60. Number of CRM policies is limited to 1 for AP 6511, ES 6510, AP 6521, and AP 621. Number of CRM policies is limited to 4 for AP 6522, AP 6532, AP 650, AP 71x1, AP 622 and RFS 4011.

61. There is a single profile for AP71XX. However, for AP 7161 and AP 7181 placement is set to "outdoor" at the device level. So even though the profile in the controller doesn't have the

"outdoor" setting, when configuration is pushed to the AP, the outdoor placement is automatically enforced.

62. Telnet is disabled on AP 621, AP 6521, ES 6510 and AP 6511, since these have limited memory.
63. On AP 6511, AP 6521, ES 6510 or AP 621, when adopted by a controller, the GUI is disabled, to make the memory available for other core functions such as additional mint routes. It is assumed that when an AP is adopted to a controller the controllers' GUI will be used for its configuration. To re-enable the GUI on these APs - use the "memory profile" parameter. Note that when an adopted AP (6521, 6511) or ES 6510 is separated from a controller to operate in standalone mode, the GUI will remain disabled due to this feature, unless the above command is used.

    If APs are already separated from the controller,
    a) Connect to AP CLI
    b) Set memory profile to 'standalone' under device override or profile context.

    If APs are currently adopted to controller then memory profile configuration change can be applied from controller CLI.
    a) Connect to Controller CLI.
    b) Set memory profile to 'standalone' under AP profile context.

    Changing the memory profile reboots the AP which then comes up with GUI.

    e.g. CONTROLLER(config-profile-default-ap6511)#memory-profile (adopted | standalone)

Introduced in a release prior to 5.4.0:

64. Wireless Controller Access protocols
    - HTTPS/SSHv2/SNMP enabled by default
    - HTTP/Telnet Disabled is by default
65. Only two (2) controllers in a cluster are supported in WiNG 5.2 and higher, the same as in WiNG v5.1.x. Cluster creation changed in WiNG v5.2 as compared to WiNG v5.1.x To create a cluster, please do the following:
    a. Controller 1 needs to be fully configured and functional
    b. For controller 2 to be added:
        - Login to Controller 1. Configure "cluster name" if not already configured.
        - Log in to Controller 2, setup an SVI with a static IP address and make sure you can ping Controller 1 IP address. DHCP is not recommended for clustering since the IP address may change later on and the cluster may not form.
        - From Controller 2, execute "join-cluster <Controller 1 IP> username "admin" and the admins' password
          rfs4000-22A3DE#cluster-join 10.10.1.1 username "admin" password "motorola"
          Joining cluster at 10.10.1.1... Done
          Please execute "write memory" to save cluster configuration.

    The requirement that user has to know the admin user name and pass word of Controller 1 makes sure that only the admin can add new controllers to the cluster. To make sure cluster config persists across reboots, user should do "write mem" explicitly after cluster is formed. The command "joincluster" changes only running-config, not startup-config.

66. When using Juniper ex2200-24p-4g or related models when connecting Motorola Access Points – either disable IGMP snooping on the Juniper switches to ensure AP adoption or configure firewall policy filter that will allow the flow of traffic to specified destination-mac-address – 01:A0:F8:00:00:00/48.

67. If using an 802.3af 10/100 power injector to power up the 802.11n APs, when plugged into a Gig E wired switch, please set link speed to 100 full, or user a GigE Power Injector.

68. Important Default Configuration Changes from 4.x to 5.x on the RFS

Description	4.x	5.x
ME1 default IP address	10.1.1.100	192.168.0.1
Auto upgrade enabled	On	On for all other platforms – controllers and AP. Disabled for the NX 9000 by default
HTTP enabled	On	Off
Default User Name/ Password	admin/superuser	admin/motorola

69. APs (& ES) have a shadow or secondary IP for gaining access to the AP if the IP address of the AP is not known but the MAC address is known. To derive the shadow IP address of an AP, use the last two hex bytes of the AP's MAC address to determine the last two octets of the IP address.

    AP MAC address - 00:C0:23:00:F0:0A
    AP IP address equivalent – 169.254.240.10

    To derive the AP's IP address using its factory assigned MAC address

    a. Open the Windows calculator by selecting Start>All Programs>Accessories>Calculator. This menu path may vary slightly depending on your version of Windows.
    b. With the Calculator displayed, selct View>Scientific. Select the Hex radio button.
    c. Enter a hex byte of the AP's MAC address. For example, F0.
    d. Select the Dec radio button. The calculator converts the F0 to 240. Repeat this process for the last AP MAC address octet.

70. Default mode for a WLAN is tunnel. For Local bridging, please change config to "local bridging".

71. WLANs created using Initial Setup Wizard are not applied to the AP300 Devices. Workaround: User needs to subsequently map these wlans for AP300 devices.

72. When experiencing high number of handshake failures in AP 300 environment it's recommended to set "wpa-wpa2 handshake priority normal" in the WLAN.

73. Features available/not available on an AP 300, when in a WiNG v5.2 or higher deployment:
    a. It is not a site survivable Access Point, and will operate as a thin port without any mesh, local bridging or forwarding capabilities- similar to WiNG v4.x and prior releases.
    b. Roaming will work in a mixed AP environment – should be on the same L2 segment.
    c. To make bulk changes to adopted AP 300s, please use Config-AP 300 {} from the CLI.
    d. Multi-country support is available for the AP 300
    e. AP 300 is not seen as a device in the tree hierarchy, but under the controllers, when the controller is the RF Domain Manager. The AP 300 cannot be an RF Domain Manager.

f. Sensor conversion from the controller is not supported. However, if the deployment is being upgraded, and the APs were previously converted to dedicated WIPS sensors for Air Defense WIPS, then they will continue to function as sensors.

g. Features not supported:
   i. Unlike the other .11n APs in WiNG v5, AP 300 continues to be a thin port with all traffic being tunneled through the controller. Will not be able to locally forward traffic
   ii. L3 Mobility
   iii. SMART RF/Self Healing
   iv. SMART Band Control will not be available
   v. No Secure WiSPe
   vi. Dual Image bank
   vii. Does not have a profile unlike the other .11n APs
   viii. Does not have the L2/L3 firewall on the AP, it resides on the controller
   ix. Sensor conversion is not available through the controller. However, if upgrading an existing installation where the AP 300 was a sensor, it would continue to be sensor, as long as it is not plugged into controller for adoption
   x. Will not support the remote packet capture like the other .11n APs in WiNG v5

74. AP adoption: APs are adopted based on valid SKUs, once discovered under the Auto provisioning policy. AP's with mismatched SKU still get adopted to the controller, but their radio does not turn on.

75. If the system flash is full from packet traces, crash files or ap-images, then there may not be enough space left on the device to create hotspot pages. If this happens, users must clear enough space from flash to allow hotspot pages to be created.

76. Radius authentication of management users uses a different configuration model from 5.0. So if upgrading from 5.0 to 5.2 or higher and you are using radius authentication for management access, you need to either change it to local authentication before upgrade, or make the mode 'fallback' and then reconfigure after upgrade using the new config model (configuring under aaa-policy).

77. Client load balancing makes decisions based on the average load in a band, in a channel within a band and average AP load. Client load balancing ignores differences in what wlans APs are beaconing. Running client-load-balancing amongst APs with different wlan config, will lead to decisions that may cause clients to NOT associate on a certain wlan

78. Install wizard is available only on the RFS 40XX, among the controller platforms.

79. In WiNG 5.x, antenna power table for the AP 650 has been updated. User should confirm power settings for the AP 650s. In 5.3, the power table for AP 6521 has been updated.

80. Multicipher support: Some of clients keep on sending deauthentication request when associated to WEP security WLAN in multicipher configuration. Please use different BSSIDs with the same WLAN, with different ciphers.

81. Commit is not allowed with radio configuration having two WLANs mapped with different data rates, as this is not a supported configuration.

82. Mesh and SMART RF – please exclude the Mesh APs from the SMART RF domain, as there may be channel changes due to RF interference that could disrupt the mesh link.

83. VPN feature has been re-implemented in WiNG 5.3 to provide a common, more optimized implementation on controllers and APs. Please use the config migration utility when upgrading from a WiNG 4.x release to WiNG 5.4.0. It is recommended that you save your old VPN config to assist in possible downgrades. Please see Note 2 on which VPN configurations

cannot be converted using the migration utility, as they are not supported in 5.3. In particular, note that configurations containing AH and DES as IKE encryption algorithm cannot be migrated. For upgrades from WiNG 5.1.x or 5.2.x to WiNG 5.4.0, the VPN config migration is performed automatically (tool is not required).

84. IPsec VPN – In comparison to VPN implementation on RFS controllers on WiNG 4.x or WiNG v5.x, here are the primary differences.
    a. Authentication Header (AH) is not supported in v5.x, but was supported in WiNG 4.x VPN. Use ESP instead of AH.
    b. L2TP over IPsec is not supported in v5.x, but was supported in WiNG4.x VPN. WiNG 5.x supports XAUTH and can be used with a IPsec VPN clients. XUATH has been tested with Cisco and Safenet VPN clients.
    c. IKEv2 was not supported in WiNG 4.x, but is supported in WiNG 5.x.
    d. DES encryption is not supported in the IKE proposal.
    e. Transport mode is only supported for host-to-host rule, in other cases it will fall back to Tunnel mode.
    f. Transport mode NAT-Traversal not supported for IKEv1 and IKEv2 in 5.x. This is supported in tunnel mode.
    g. In the case of IKEv1, if PFS option for IPSec SA (under crypto map entry) is configured on both peers, then the value requested by the initiator is used for the tunnel. If the configured PFS value on the initiator end is lower than that configured on the responder, the lower value is used. If PFS is required, please configure the same PFS value in both the peers.
    h. The value of Kilobyte expiry of an IPSec SA (security-association lifetime kilobytes) can be configured to as low as 500KB. This has to be used with caution. If there is a lot of traffic on the tunnel and the value is set to very low value, the tunnel will end up in an indefinite rekeying IPSec SA state. This value has to be arrived at based on the maximum traffic that is expected on the tunnel and set such that there is an interval of at least a few minutes between rekeys. It is recommended that this value be set to a minimum of 512000 (500MB).
    Impact from lack of the above 4.x features if any, is expected to be minimal.

85. IPsec VPN statistics - following SNMP tables are not available for VPN statistics via SNMP – they will be implemented in a future release – wingStatsDevVpnIpsecSaTable, wingStatsDevVpnIpsecSaTrafficSelectorTable, wingStatsDevVpnIkesaTable

86. Built-in RADIUS server is available as a demo capability on AP 6521 and can be configured via CLI.

87. Auto-tunnel for VPN
    a. A single group id/PSK is supported on RFS controllers. All APs use same group id/PSK.
    b. When APs are behind NAT (e.g. two remote sites), it is required that the AP IP address are different.
    c. Auto IPsec tunnel termination has been verified on Cisco Gateways with PSK/RSA authentication.

88. VRRP
    a. VRRP version 3.0 (RFC 5798) and 2.0 (RFC 3768) are supported. Default is version 2 to support interoperability. Please note that only version 3 supports sub-second failover.
    b. Services like DHCP, RADIUS, NAT, and VPN running on the virtual IP are supported
    c. For DHCP relay, you can point to the DHCP server as virtual IP
    d. For VPN, on the initiator side, remote peer can be configured as virtual IP

89. If using TFTP to upgrade an AP 6521, AP 6511, ES 6510 or AP 621, on the TFTP server please configure the following settings:
    a. Per packet timeout in seconds: 15
    b. Maximum retries: 20
90. When using iPods as clients, you may see WPA2 group key rotation handshake failures while MUs are idle (2.4GHz band). Change the handshake timeout to 2 sec to correct this problem. From the wlan config, the cli command is: wpa-wpa2 handshake timeout X (where X is the timeout in ms, within a range of 10-5000)
91. Auto assign sensor is not available for AP 6511, AP 6521, ES 6510 or AP 621 – since this feature requires a reboot on low memory devices, which cannot be done with Smart RF enabled.
92. For IGMP Snooping version v2, v3, source specific multicast is not supported, this will be addressed in a future release.
93. To safeguard against unknown attacks, it is recommended that management access be restricted to authorized hosts/subnets. This can be done using the restrict-mgmt-access host/subnet cli command under management-policy.
94. RFS 7000 - Compact flash card will not work on pre-Rev F RFS 7000 hardware.
95. NX 9XXX:
    - NX 9000 requires a laptop with a minimum of 4GB RAM for viewing GUI with greater than 3000 AP.
    - Extended VLANs are not supported on the NX 9000/NX 9500. Only Local VLANs are supported.
    - There is no VPN, or Advanced WIPS support on the NX 9000/NX 9500.
96. AP 7131: PoE and Gigabit Ethernet Ports:
    The AP 7131 family features upgraded Gigabit Ethernet (GE) ports. These ports are labeled as follows:

    - GE1/PoE: GE1 is the LAN Port and supports 802.3af, 802.3at (draft) PoE.
    - GE2: GE2 is the WAN port.

    Single radio models can operate fully with 802.3af power sources. Dual radio models and tri-radio models can also power up two radios and GE1 interface with 802.3af power sources. At higher power levels, 2 radios and both Ethernet interfaces are fully functional in the dual and tri-radio models. Single, dual and tri- radio models can also operate using an A/C power supply. The third radio (dedicated WIPS sensor radio or a future modular off-the-shelf 3G WAN Express Card) on the tri-radio model requires 802.3at power levels, A/C power supply or a Gigabit Ethernet PoE+ injector.

    The following table shows the radio and LAN resources available under various power configuration modes for the AP 7131 family:

Available Power	Radio Resources	Ethernet Port Configuration
Power Status: 3af (12.95W)	2 Radios	GE1 10/100/1000
Power Status: 3at (24W)	3 Radios (Express Card option supported with radios at lower power)	GE1 10/100/1000 GE2 10/100/1000
Power Status: Full Power (30W)	3 Radios (with Express Card)	GE1 10/100/1000 GE2 10/100/1000

When a Motorola 802.3af power injector (AP-PSBIAS-1P2-AFR) is used with AP- 7131 or AP 7131N, then the GE1 or LAN1 port will be limited to 10/100 Mbps. Motorola recommends the 802.3at (Draft) power injector (AP-PSBIAS-1P3-AFR) to be used with AP 7131/AP 7131N configurations.

97. When AP adopts to Controller, the clock is not getting sync with controller clock immediately. It happens over period of time depending on time delta.

6. Important Notes for Analytics

- Analytics only supported on NX 95XX series of controllers.
- Analytics is only supported on a cluster when running active-standby mode.
- Changes to enable on-board analytics on WLAN – “http-analyze” under WLAN profile.
- When working in cluster – following firewall ports need to be opened:

  tcp - 8020, 50010, 50020, 60000, 60020, 2181 (proprietary protocol)
  tcp - 50070, 50090 (http is used on these ports)
  tcp - 50075, 60010, 60030 (also via http, carry debug related traffic)
- The nodes in a cluster must be configured to use NTP. The skew must be not less than 15 seconds
- Take a backup of the analytics database on each controller before upgrade and on a regular basis. If for any reason data becomes corrupted – it can be restored from last back up.
  1. <u>When upgrading from WiNG 5.4.3 or higher</u>
     To back up everything including database:
     service copy analytics-support ftp://<ip address of server>/<name of file>
     To restore database:
     archive tar /xtract ftp://<ip address of server>/<name of file> /
  2. <u>When upgrading from WiNG 5.4.1/ 5.4.2</u>
     Open a browser and enter the URL:
     https://<primary_ip>/stats/dsr/backup/backup_download?stream=true&
     ticket=nx2nx2
     The above URL will download the analytics data into local file system
- When upgrading from WiNG 5.4.x to 5.5, data from WiNG 5.4.x is migrated over to WiNG 5.5. When downgrading from 5.5 to 5.4.x, the system does NOT bring back data from 5.5 to 5.4.x. This means the user will revert to the previous WING 5.4.x backup data.
- Configure your new systems after the upgrade:
  - ✓ On the Primary controller
    - ○ service analytics primary <primary_ip>
    - ○ enable analytics in the device or profile context (cli command is “analytics”)
    - ○ commit write memory
  - ✓ On the Standby controller:
    - ○ service analytics clear-data
    - ○ service analytics secondary <secondary_ip> <primary_ip>
    - ○ enable analytics in the device or profile context (cli command is “analytics”)

  - commit write memory

NOTE: If you do not enter the above CLI commands, then Analytics starts as Standalone on both systems.

- Due to removal of license requirement – new command has been added to enable/disable analytics.

```
nx9500-6C8647(config-device)#analytics?
    analytics  Enable WiNG Onboard Analytics Data
```

Analytics will no longer be started by default, but will be enabled by this device/profile configuration parameter. Also, wifi data polling will be enabled with analytics (cannot be controlled separately). Upon upgrade to WiNG 5.6 – user must configure to enable analytics to continue to use this feature.

7. DFS Tables, Sensor and Radio Share

1. Following is the DFS support in WiNG v5.6 for the supported radio platforms:

Product	Master DFS FCC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS ETSI	Client DFS Japan
AP 650 /6532	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 713x	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7161	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7181	Disabled	Enabled	Enabled	Disabled	Enabled	Enabled
AP 6511	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 621 /6521	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 622/6522 /6562	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 8132	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 8122/ 8163	Enabled	Enabled	Disabled	Enabled	Enabled	Disabled
MOD-8132-6001S-WW	NA	NA	NA	Enabled	Enabled	Enabled
AP 8222/8232	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled
RFS 4011	Disabled	Disabled	Enabled	Disabled	Disabled	Enabled

98. Air Defense sensor capabilities are supported on all the 802.11n APs in this release, and are available for enabling the WIPS functionality as well as the Network Assurance Capabilities. There are some caveats on managing the AP directly via ADSP, for certain AP platforms:

Network Assurance Toolset when Radio is dedicated as a sensor	**AP 621 651 6521** (Note 1)	**AP 650**	**AP 622**	**AP 6532**	**AP 6522 6562**	**AP 7131 7161 7181**	**AP 8132 8122 8163**	**AP 82XX**
Spectrum Analysis	No	Yes	No	Yes	No	Yes	No	No

Advanced Spectrum Analysis	Yes	No	Yes	No	Yes	No	Yes	No
Live RF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Live View	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
AP Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Connectivity Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Note 1: GUI is disabled and number of SSH sessions is limited to 1

99. Radio Share functionality (allows for enabling the Network Assurance toolkit in ADSP, without dedicating a radio as a sensor) is available on all the 802.11n APs with some caveats – please see details below:

Network Assurance Toolset with Radio Share	**AP 6511 621 6521** (Note 1)	**AP 650**	**AP 622**	**AP 6532**	**AP 6522 6562**	**AP 7131 7161 7181**	**AP 8132 8122 8163**	**AP 82XX**
Spectrum Analysis	No (Note 2)	No (Note 2)	No (Note 2)	No (Note 2)	No (Note 2)	No (Note 2)	No	No
Advanced Spectrum Analysis	Yes	No	Yes	No	Yes	No	Yes	No
Live RF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Live View	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
AP Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Connectivity Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Note 1: GUI is disabled when Radio Share is enabled
Note 2: Spectrum Analysis is not supported with Radio share enabled.

8. Issues Fixed

SPR #	Description
23997	Cleaning wireless WIPS blacklist does not work immediately.
24339	TACACS + Authorization Fallback is not available, user's cannot run CLI commands.
24970	Captive portal fail page does not appear if incorrect username is entered.
25068	Legacy mesh tab is missing from GUI on AP6522 5.5 standalone.
25095	Constant reboot occurs when adding 3rd WLAN to Radius Policy/Authentication and commit/save.
25096	CP redirect url throws error when aaa/cp policy name includes 'z' character (IOS devices only)
25103	wrong command for Single Hop Mesh in techdump
25108	static entry is getting removed from dns snoop table, causing too many redirect for external portal request
25111	On AP 6511 large MAC address table causes hang in terminal session
25114	Initial Setup Wizard re-appears after going through the wizard process the first time and completing the comm
25136	All existing IPSEC tunnels go down when ACL rules for a crypto map is reached the limit
25139	Data collection from remote RFDMs should be removed from tech-support command logic
25144	Wing 5.5.x device send Client ID in the DHCP request instead of the hardware address
25197	When Exclude WPA2-TKIP is enabled with both WPA/WPA2-TKIP and WPA2-CCMP enabled, WPA2-CCMP clients can't connect
25242	DHCP policy can’t be activated in GUI on standalone AP
25243	OK button grayed out if you try to add APs through pending adoption section.
25244	Device type not recognized when adding through pending adoptions.
25245	Fast BSS Transition on open WLAN causes RIM crashes
25254	Reset to Factory defaults is not removing all files from file system - history, licenses are maintained
25283	techsupport attempts to collect VM data and dsk image, grows over 100GB.
25284	APs not getting adopted when ‘preferred-controller-group’ is configured with cluster pair as controller hosts
25288	show captive portal sessions filter is not working
25316	SNMP trap for AP un-adoption is not working
25350	“Control Vlan” configurable option under device overrides should be removed from GUI. Command not available in CLI
25351	Device has a low memory dump with rim process showing high memory usage.
25386	PDT6846's fail to automatically re-connect to network after resume without rebooting device.
CQ 105186	DFS: AP8232 does not return to its original configured channel.
CQ 108001	Management, data and control frames RSSI values shows -111 in outbound subscriber
CQ 107821	AP 8132 stops beaconing on 2.4ghz radio frequently
CQ 108333	Qualys Security Scan reports new NTP Denial of Service Vulnerability

CQ 108961	Site controller should recover from config push from NOC controller that potentially causes it to lose connectivity to NOC
CQ 197406	CDP/LLDP Port information Update - Removed periodic update of CDP/LLDP port information update from adopted devices to controller to only when the port information changes on the adopted device
CQ 197514	When an RFS 7000 deployed as a site controller is adopted to an RFS 7000/ NX 95xx NOC controller is downgraded from WiNG 5.6 to WiNG 5.5 the RFS7000 may crash. Workaound: Use "boot system *primary/secondary*" to switch to the backup partition and reload the controller.
CQ 197593	In AP 7131 deployments where tunneled VLAN is configured also on physical port of the AP, presence of Bonjour enabled device can cause if broadcast flood.

9. Known Issues

New in WiNG 5.6:

CQ/ SPR	Headline	Comments
SPR 25274	Floorplan disappears when you get down to AP/client level	
SPR 25338	Cfgd error dpd2/actions.py:78:get_dict_from_dpd2 cmd=22 param='* and dpd2 crash seen	
SPR 25343	Caller-Id field in the TACACS packets sent to ACS should use the IP-Address of the host trying to login	
SPR 25377	PSP state between AP and MC 3090 frequently goes out of sync when AP is using SMART-RF	
CQ 107523	AP 6521/ AP 6511 – when using 3rd party certificate with 1028 bits or less – on upgrade to WiNG 5.5.1 will experience dpd2 crash.	
CQ 107805	Commit Warning appears when accessing Step By Step Wizard under VPN security wizard	Happens only with the step-by-step wizard. Commit and move forward. Will be addressed in a future release.
CQ 108125	Stage the T5 with vlan1 IP only. Customer will need do extra configuration in the T5 profile if planning to have a different non-vlan1 Management Vlan.	
CQ 108286	Client load balancing - Inconsistency in CLI/GUI default behavior	
CQ 108303	IPX - T5 console hangs after deleting the private CPE vlan4090.	Create vlan4090 from WiNG 5, you can then delete it or modify it if required. After the T5 gets adopted to a WiNG 5 controller, all subsequent configuration should be done from WiNG - do not configure directly on on the T5 switch (unless you are configuring features are not yet supported on WiNG).
CQ 108357	AP 7161: Mesh-ACS restarts on non root APs when rf-mode 5ghz is mapped to radio index 1 and meshpoint is mapped to it. This issue is caused by invalid configuration – there is a	Will be addressed in a future release.

	invalid channel in the channel list. Workaround: Remove the invalid channel from the channel list.	
CQ 108470	Wired captive portal: Login from a redirected page for an expired session fails to go through. Relogin from a new browser window	
CQ 108606	Bonjour_Gateway: Apple clients are not able to see/access iTunes Bonjour services	Will be addressed in a future release.
CQ 108653	GUI: RF Domain Device Upgrade status - history is not displayed correctly for each RF-Domain.	Will be addressed in a future release.
CQ 109068	When AP Adoption steering feature is used, infrequent AP reboot is seen for AP 621 and AP 6521 only. Not applicable to other APs.	
CQ 197351	MAP00197351 - IPX - CLI auto-provisioning-policy redirect has option for T5 which cannot participate in this redirect design	This relates to the new Controller steering feature in 5.6, which is not supported for T5. The CLI command will be updated in a future release to remove the option for the T5 switch.
CQ 197480	$AUTO-RF-DOMAIN option missing in NX 95XX GUI under adoption policy	Workaround: Use CLI. Will be addressed in a future release.
CQ 197579	Following message seen when NAT Traversal is configured. %AUTHPRIV-4-WARNING: pluto[852]: including NAT-Traversal patch (Version 0.6c)	No functional impact
CQ 197608	AP Adoption Steering is not supported with Hierarchical Management. The steering controller should be independent (i.e. should not be adopted to another NOC controller).	Will be addressed in a future release.
CQ 197705	NX 95xx – following error message is seen on upgrade- %USER-4-WARNING: RAID: megacli command failure (-AdpEventLog -GetEvents -f /flash/archived_logs/megraid.log -a0 -NoLog) returned 'AdpEventLog failedFW error description:The requested command cannot be completed as the specified object does not exist.Exit Code: 0x23'	No functional impact. Ignore the message.
CQ 197778	When user import any configuration into the Startup-config from GUI (Deskboard) using "local", it looses it's formatting.	No functional impact. Displays properly when saved externally.
CQ 198140	Meshconnex – setting both radios to operate on the same band and same channel does not work.	This is not supported.
CQ 198454	Changing channel to static configuration, during acs calibration takes effect only after the radio has finished calibration (Duration ~30 seconds)	

From WiNG 5.5.x releases.

CQ/ SPR	Headline	Comments

CQ 92952	VM hangs while installing Fedora 17, 32-bit.	Workaround: When booting fedora 17 (Fedora-17-i686-Live-Desktop.iso), select "Troubleshooting" then "Start Fedora 17 in basic graphics mode". With that the VM installs correctly.
CQ 92965	VM: VNC does display after installing redhat enterprise desktop version 6.4.	Solution is to pick the basic graphic driver during install.
CQ 93019	Content caching does not work when NX45xx/65xx is behind a proxy server.	The NX 45xx/ 65xx needs to be configured as the proxy server.
CQ 93053	Mesh: When using meshpoints with 5.4.1 or higher with a WLAN controller running firmware prior 5.4.1 will not adopt the non-root meshpoints.	The network stays up and will re-adopt once the controller is upgraded to 5.4.1 or higher.
CQ 93308	Mesh: When a radar is detected by a radio the channel has to be vacated for 30 minutes. With the rehome feature turned on by default, the radio goes back to the original channel after 30 minutes of inactivity timeout. This feature is not compatible with a mesh network and causes network instability.	To avoid this, use the command no dfs rehome command.
CQ 93582	VM Management GUI: VM dashboard https VNC to third-party VM does not always work.	This is an issue related to specific third party VMs and cannot be fixed in WiNG.
CQ 97758	Dynamic Mesh: Message seen: Reloading: Lost connectivity with controller after config update (user: connection-monitor)	Workaround: Since dynamic mesh can go into states of adoption and un-adoption you need to set the following: misconfiguration-recovery-time 0
CQ 98642	ONEVIEW: The “CFG STAT” column is the status of the last configuration push to the device. When a site controller adopts to a NOC controller, the NOC sends the full site configuration to that controller. This causes the site controller to show up as "configured". When configuration changes are made, the NOC sends the changes only to the site master (and skipped for other adopted controllers in the same site). The skipped controllers “CFG STAT” is set to 'cluster-member' to indicate that they were skipped.	
CQ 100882	The Flash size on RFS platforms is 84MB. Due to this, only three access point images can be loaded at a time.	Once the access points are upgraded the user has to delete one or more images to make space to upgrade additional AP types.
CQ 103815	Some wireless clients cannot associate on DFS channel after radar scan.	This is a client issue seen for the following clients: Netgear A6200, D-Link DWA-182
CQ 103922	Error message on console after upgrade "EXT4-fs (sda7): ext4_da_writepages: jbd2_start: 8192 pages, ino 2365565; err -30"	Ignore, has no functional impact. Will be addressed in a future release
CQ 104544	AP 82xx: Configuring unsupported features may result in poor performance.	
CQ 104846	AP 82xx: Advanced items under radio properties not configurable	

CQ 105252	Dynamic VLAN assignment with Captive Portal: Client should get the IP address from pre-auth VLAN on captive portal inactivity timeout.	Workaround: On a captive portal inactivity timeout the client stays on the post auth-vlan but will have to re-login (just like if the client was returned to the pre-auth vlan). If the MU inactivity timeout expires, client will be returned to the pre-auth VLAN.
CQ 105294	Interoperability: Macbook Air(11ac) shows reduced throughput performance for upstream/downstream traffic. We observed an impact on the throughput at the beginning of the test.	The issue is on the client side. The same test produced expected results with the Asus 3x3 module.
CQ 105922	Netgear Client A6200 interoperability issues with AP82xx access points. The client goes into a re-connectivity loop in WPA2-AES mode.	Workaround is to reload the client.
CQ 106338	snmp-server display-vlan-info-per-radio" does not work correctly	Will be addressed in a future release.
CQ 107523	AP 6521/ AP 6511 – when using 3rd party certificate with 1028 bits or less – on upgrade to WiNG 5.5.1 will experience dpd2 crash.	Will be addressed in a future release. Functionality is not impacted. It's advisable to install certificates with 2048 bit or higher prior to upgrade.

From WiNG 5.4.x or prior releases.

CQ/SPR	Headline	Comments
CQ 82675	Remote VPN IKEV2: Remote VPN client that is assigned a Virtual IP from ext DHCP server is not able to ping SVIs but is able to ping wired hosts/wireless clients.	
CQ 82794	AP 6521 upgrade fails with both Smart-RF and Radio Share enabled simultaneously.	Workaround is to disable Radio Share to perform the upgrade.
CQ 82918	NX 65XX/45XX: T1/E1: Switch changes states of all T1 interfaces even if one serial interface configuration is changed	Any configuration change to a T1 or serial interface will result in a restart of all T1 interfaces.
CQ 83297	NX 65XX/45XX Cannot import/export VM configurations (VM config is not maintained in WiNG)	VM related configuration will not be displayed in the running-config. Execute "show virtual-machine configuration" to view VM configuration
CQ 83731	L2TPv3: "show L2TPv3 tunnel <tab>"CLI does not show configured tunnels.	Workaround: show L2TPv3 tunnel-summary
CQ 85745	Smart-RF for MCX: WiFi Interference recovery does not work.	Work around: Manually trigger a scan on a root device as required.
CQ 86334	AP Wizard does not auto launch in some cases.	Workaround: Clear browser cookies.
CQ 86584	Radio share is not supported on domain manager AP.	
CQ 86814	When using critical resource monitoring over a specific port, some devices will not respond to the ARP requests with a 0.0.0.0 source address.	In this case, 'service critical-resource port-mode-source-ip' should be used. To prevent ARP cache poisoning, a _different_ IP from the device IP address must be used.

CQ 86933	There is a limit of one CRM policy for a Mesh Point.	
CQ 87177	Shutdown on meshpoint loss does not work for tunneled wlans when critical resource goes down.	Workaround is to “Shutdown on unadoption”
CQ 88049	Smart-RF for MCX: Interference recovery triggers when we configure mismatching channel widths.	Workaround: Channel width on non-roots should match with the root or should be set to auto
CQ 88334	A mesh adopted AP with a WLAN using 'shutdown on-unadoption' mapped to the same radio may get un-adopted. Controller timeouts on the AP should be increased to maintain adoption.	The following are recommended minimum values for an AP in this use-case: 'controller hello-interval 30' and 'controller adjacency-hold-time 40'.
CQ 88432	NX 9500+Analytics: Search terms not captured if searched on tablets PC using prefix ‘m’. (e..g m.bing.com). Results are correctly captured if this type of access is performed from cell phones. When the m prefix is used on tablets, it generates URLs with Active X script requests which are not supported.	
CQ 89625	GUI: mesh visualization view goes outside the screen.	Drag the image to see the complete view.
CQ 90125	Cannot connect to AP 6521/AP 6511 via MINT from the controller.	Workaround: disable telnet in the management policy.
CQ 90275	GUI: firwware upgrade via ftp option does not abort if abort button is pressed	
CQ 91319	Spectralink: after enabling accelerated multicast, PTT doesn't go to all the handsets.	When using PTT – disable accelerated multicast.
CQ 97410	If the ipsec-secure L2TPv3 tunnel is terminated on the vrrp address then the reply packet is un-encrypted from the concentrator	Work around is to configure the "local-ip-address” in the L2TPv3 concentrator.
CQ 98002	When traffic hits ACL, hit-counter is not updated.	